

(19) 世界知的所有権機関
国際事務局



(43) 国際公開日
2001年2月22日 (22.02.2001)

PCT

(10) 国際公開番号
WO 01/13293 A1

(51) 国際特許分類: G06F 17/60

(21) 国際出願番号: PCT/JP00/05439

(22) 国際出願日: 2000年8月14日 (14.08.2000)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願平11/228154 1999年8月12日 (12.08.1999) JP

(71) 出願人 (米国を除く全ての指定国について): 松下電
器産業株式会社 (MATSUSHITA ELECTRIC INDUS-
TRIAL CO., LTD.) [JP/JP]; 〒571-8501 大阪府門真市
大字門真1006 Osaka (JP).

(NAKANISHI, Yoshiaki) [JP/JP]; 〒166-0014 東京
都杉並区松ノ木2-4-10-305 Tokyo (JP). 高山 久
(TAKAYAMA, Hisashi) [JP/JP]; 〒156-0043 東京都
世田谷区松原5-6-12 Tokyo (JP). 松瀬哲朗 (MAT-
SUSE, Tetsuo) [JP/JP]; 〒565-0853 大阪府吹田市春日
2-6-3-109 Osaka (JP).

(74) 代理人: 弁理士 蔵合正博, 外(ZOGO, Masahiro et
al.); 〒102-0083 東京都千代田区麹町5丁目7番地 秀和
紀尾井町TBRビル Tokyo (JP).

(81) 指定国 (国内): CN, JP, KR, US.

(84) 指定国 (広域): ヨーロッパ特許 (DE, FR, GB).

添付公開書類:
— 国際調査報告書

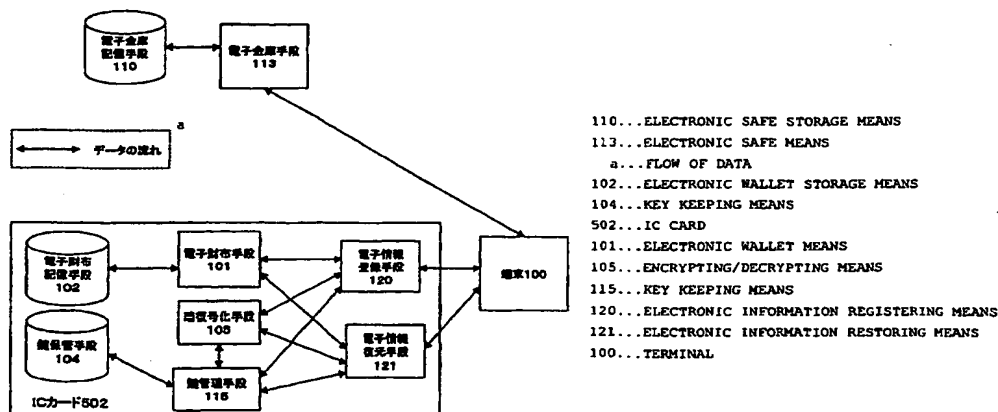
(72) 発明者: および

(75) 発明者/出願人 (米国についてのみ): 中西良明

2文字コード及び他の略語については、定期発行される
各PCTガゼットの巻頭に掲載されている「コードと略語
のガイダンスノート」を参照。

(54) Title: ELECTRONIC INFORMATION BACKUP SYSTEM

(54) 発明の名称: 電子情報バックアップシステム



(57) Abstract: An electronic information backup system for safely back up electronic value information about electronic money and electronic ticket through communication in a server so as to exclude unauthorized actions when backup and restoring are performed and for restoring the electronic value information from the backup in case of emergency such as loss of key information. In this system, electronic value information is encrypted, the encrypted electronic value information is registered in an electronic safe server, and the user receives the registration, presents the registration to the server to receive the encrypted electronic value information, and decrypts the electronic value information with decrypting key data. The decrypting key can be kept in another server. The electronic value information and the decrypting key can be kept separately in different servers. It is possible to keep the sequence of number of the cryptogram to serve as the basic the decrypting key in the server, and to generate a decrypting key according to a decrypting key generation algorithm on the terminal side. In case of loss of the decrypting key, the possessor certificate information is verified and then the user can receive the decrypting key from the server.

[続葉有]

WO 01/13293 A1



(57) 要約:

通信を介してサーバ上に電子マネーや電子チケット等の電子価値情報を安全にバックアップし、バックアップと復元の際に不正行為を排除し、鍵情報消失などの緊急時に電子価値情報をバックアップから復元する電子情報バックアップシステムを提供する。このシステムでは、電子価値情報を暗号化して電子金庫サーバ上に登録してその登録証を受け取り、後に、登録証をサーバに提示して暗号化電子価値情報を受け取り、データ化された復号鍵で復号する。復号鍵は別のサーバに預けてもよい。また、電子価値情報及び復号鍵を分割して、別々のサーバに預けてもよい。また、復号鍵の元となる暗号の数値をサーバに預け、端末側ではそれを復号鍵生成アルゴリズムを用いて復号鍵に生成してもよい。復号鍵を紛失した場合は、所有者認証情報を検証した後、サーバから復号鍵を受け取ることができる。

明 細 書

電子情報バックアップシステム

技術分野

本発明は、コンピュータと情報通信を用いたバックアップシステム、特に電子現金や電子チケットといった電子価値情報のバックアップと復元を行なうシステムに関するものである。

背景技術

電子現金や電子チケットなどの金銭もしくは金銭的価値のある情報を、電子的な形式で表現し利用する技術が一般的となってきた。電子現金や電子チケットなどの電子的に表現された価値情報を、以下、電子価値情報とする。

電子価値情報の実現方法の一つとして、遠隔地のサーバ上で電子価値情報を置き、その所有者は認証情報のみを持ち、利用時にサーバと通信するようにする方法がある。前記の方法では、認証の安全性を確保する事によって安全な取り引きを実現できるが、ネットワークに接続できる状態でなければ電子価値情報を使用できないという問題や、ネットワークへの問い合わせが使用の度に発生するため、高速な反応を要求する状況には適用しにくいという問題がある。

そのため、ネットワークと独立した状態でも電子価値情報を利用することが出来るように、電子価値所有者の持つICカード、携帯電話、携帯端末などのデバイス上に電子価値情報そのものを保持するようにする技術も存在する。ただしこの場合、デバイスの破損や紛失によって電子価値情報が消失してしまう危険性を持っている。

上記の電子価値情報を含む電子情報の破壊という問題からの回復を実現するため、従来いくつかの技術が考案されている。以下にその例を示す。

第一の従来技術として、特開平10-133925号公報に示される技術では、暗号化したメールを用いることで、ファイヤーウォール内から外のバックアップサーバに対してデータのバックアップを行う。ただしこの技術では、鍵の紛失や破損時に暗号化したデータからの復元方法については考慮されていない。

第二の従来技術として、米国特許5、778、395に示される技術では、ネ

ットワークに繋がったノード(コンピュータ)のファイルを別のノード上のサーバに圧縮や暗号化を行ってバックアップする。ただしこの技術でも、第一の従来技術と同様に鍵の紛失や破損時のことが考慮されていない。

上述のように、従来技術は、暗号によって秘匿した状態で電子情報のバックアップと復元を行うものであった。しかし、従来技術では、暗号に用いた鍵情報が消失した場合に暗号化されたバックアップ情報を復元することについて考慮されていないため、鍵情報も含めた電子情報を格納したデバイスの紛失や破壊などに対処できないという問題がある。

また、上記の問題に対応するために暗号の復号に用いる鍵を単純にバックアップしたとしても、鍵を預けたサーバと暗号化した電子価値情報を預けたサーバの両者が共謀するなど、鍵のバックアップ管理の信頼性を損なうような不正行為に対しても対処しなければならない。

発明の開示

本発明の目的は、通信を介してサーバ上に電子価値情報を安全にバックアップすることと、バックアップと復元の際に不正行為を排除することと、鍵情報消失などの緊急時に電子価値情報をバックアップから復元することを可能とする電子情報バックアップシステムを提供することにある。

本発明によれば、電子価値情報を暗号化して電子金庫サーバ上に登録してその登録証を受け取り、次に、登録証をサーバに提示して暗号化電子価値情報を受け取り、データ化された復号鍵で復号するシステムが提供される。復号鍵はユーザが持っていてよいし、サーバに預けてもよく、さらに、別のサーバに預けてもよい。また、電子価値情報を分割し、さらには復号鍵をも分割し、両者を一体に或いは部分的に一体にサーバに預けるか、またはまったく別々のサーバに預けてもよい。また、復号鍵の元となる暗号の数列为サーバに預け、端末側ではそれを復号鍵生成アルゴリズムを用いて復号鍵に生成してもよい。復号鍵を紛失した場合は、所有者認証情報を検証して検証が成功すれば、サーバから復号鍵を受け取ることができる。

図面の簡単な説明

第 1 図は、本発明の実施の形態 1 における電子情報バックアップシステムの構成図である。

第 2 図は、本発明の実施の形態 1 における電子価値情報とダイジェスト情報と登録証の模式図である。

第 3 図は、本発明の実施の形態 1 における電子財布手段上での電子価値情報と登録証の管理方法を示す模式図である。

第 4 図は、本発明の実施の形態 1 における電子金庫記憶手段での情報保管方法を示す模式図である。

第 5 図は、本発明の実施の形態 2 における電子情報バックアップシステムの構成図である。

第 6 図は、本発明の実施の形態 2 における登録電子価値情報と登録証の模式図である。

第 7 図は、本発明の実施の形態 2 における鍵保管手段上での暗号鍵と復号鍵の保管方法を示す模式図である。

第 8 図は、本発明の実施の形態 2 における鍵管理記憶手段上の鍵情報の管理方法を示す模式図である。

第 9 図は、本発明の実施の形態 2 における電子金庫記憶手段での情報保管方法を示す模式図である。

第 10 図は、本発明の実施の形態 3 における電子情報バックアップシステムの構成図である。

第 11 図は、本発明の実施の形態 4 における電子情報バックアップシステムの構成図である。

第 12 図は、本発明の実施の形態 5 における電子情報バックアップシステムの構成図である。

第 13 図は、本発明の実施の形態 6 における電子情報バックアップシステムの構成図である。

第 14 図は、本発明の実施の形態 7 における電子情報バックアップシステムの構成図である。

第 15 図は、本発明の実施の形態 8 における電子情報バックアップシステムの構成図である。

第 16 図は、本発明の実施の形態 9 における電子情報バックアップシステムの構成図である。

第 17 図は、本発明の実施の形態 10 における電子情報バックアップシステムの構成図である。

第 18 図は、本発明の実施の形態 11 における電子情報バックアップシステムの構成図である。

第 19 図は、本発明の実施の形態 11 における電子財布記憶手段上の電子価値情報群を示す模式図である。

第 20 図は、本発明の実施の形態 11 における電子財布記憶手段上の電子価値情報群を示す模式図である。

第 21 図は、本発明の実施の形態 12 における電子情報バックアップシステムの構成図である。

発明の好ましい実施の態様

本発明は、第 1 に、ローカルの電子価値情報を電子金庫サーバ上に登録してその登録証を受け取り、その登録証を電子金庫サーバに提示することにより、対応する電子価値情報を取得できるようにしたものである。これにより、ローカルの電子価値情報が破損した場合でも電子価値情報を復元することが可能になる。

本発明は、第 2 に、ローカルの電子価値情報を暗号化して電子金庫サーバ上にバックアップする。これにより、電子価値情報を電子金庫サーバに隠蔽した状態でバックアップすることができ、ローカルの電子価値情報が破損した場合でも電子価値情報を復元することが可能になる。

本発明は、第 3 に、暗号化した電子価値情報を復号化するための復号鍵を異なる電子金庫サーバにバックアップする。これにより、電子価値情報をより安全に保管することが可能になる。

本発明は、第 4 に、電子価値情報を分割してそれぞれを異なる電子金庫サーバにバックアップする。これにより、バックアップ時の全通信路の傍受や、全電子

金庫サーバへの不正侵入を行うなど、不正に前記復号鍵を取得する困難度が高くなる。また、それぞれの電子金庫サーバの独立性が高ければ、電子金庫サーバ管理者の共謀による復号鍵の不正な復元が行われる可能性を低くすることができる。

本発明は、第5に、複数の電子価値情報を結合して暗号化し、電子金庫サーバにバックアップし、電子金庫サーバから取得した時に結合を分離して電子価値情報を復元する。これにより、バックアップ時の全通信路の傍受や、全電子金庫サーバへの不正侵入を行うなど、不正に前記暗号鍵を取得する困難度が高くなる。また、それぞれの電子金庫サーバの独立性が高ければ、電子金庫サーバ管理者の共謀による復号鍵の不正な復元が行われる可能性を低くすることができる。

本発明は、第6に、復号鍵を分割して、一方の分割鍵を電子価値情報とともに一方の電子金庫サーバにバックアップし、他方の分割鍵を他方の電子金庫サーバにバックアップする。これにより、バックアップ時の全通信路の傍受や、全電子金庫サーバへの不正侵入を行うなど、不正に前記暗号鍵を取得する困難度が高くなる。また、それぞれの電子金庫サーバの独立性が高ければ、電子金庫サーバ管理者の共謀による復号鍵の不正な復元が行われる可能性を低くすることができる。

本発明は、第7に、復号鍵を数学的に生成するために用いる元の暗号種（たね）情報を電子金庫サーバにバックアップし、復元時に暗号種情報を電子金庫サーバから受け取り、暗号種情報から復号鍵生成アルゴリズムを通して復号鍵を生成する。これにより、電子価値情報のみならず、復号鍵の安全性が極めて高くなる。

本発明は、第8に、所有者情報と認証情報とを照合して一致した場合に電子金庫サーバから電子価値情報を取得可能とする。これにより、復号鍵を紛失したり、端末が破壊されてデータが取り出すことができない場合でも、電子金庫サーバから復号鍵を取得して電子価値情報を復元することができる。

本発明は、第9に、予め設定したバックアップ条件に従って電子価値情報を選択する。これにより、バックアップする電子価値情報の選択を、ユーザによる手動選択ではなく事前に設定した条件に基づいて自動的に行なうので、ユーザの負担を軽くすることができ、端末のメモリ容量や通信にかかるコスト（時間、費

用)を抑えることができる。

本発明は、第10に、安全のために電子価値情報と復号鍵を別の電子金庫サーバに預けた場合に、認証によって正当な情報保持者と認定された場合には、電子金庫サーバ同士が通信を行なって、電子価値情報と復号鍵とを合わせて送り返してくるので、復号鍵を紛失した時や端末が破壊されてデータを取り出すことができない時でも、電子価値情報を復元することができる。また、電子価値情報を直ぐに利用しない場合は、新たな暗号鍵を用いて電子価値情報を暗号化し、それを一方の電子金庫サーバに送るとともに、復号鍵を他方の電子金庫サーバに送ることにより、従前の状態に戻すことができる。

実施例

以下、図面を用いて本発明の実施例について説明する。なお、本発明はこれらの実施例に何ら限定されるものではなく、その要旨を逸脱しない範囲に置いて種々の態様で実施し得る。各図は図1、図2・・・のように表示する。

実施例1

図1、図2、図3、図4を用いて、本発明の請求項1、2、3に係る第1の実施例について説明する。図1は本実施例1が示す電子情報バックアップシステムの一例を示した構成図である。本システムは基本的に有線または無線の通信路によって結ばれたコンピュータ装置と、それに接続された外部拡張機器およびそれらの上で動作するソフトウェアで構成されるものとする。ここでいうコンピュータ装置とは、ソフトウェアプログラムに従って動作する中央演算装置を備えた機器の総称を意味するものとする。

本実施例1では、電子財布手段101および電子財布記憶手段102および電子情報登録手段106および電子情報復元手段107は、ICカード501内に構成される。端末100は、ICカードリーダー・ライタを備えた携帯電話端末であり、ICカード501内に構成された電子情報登録手段106および電子情報復元手段107と通信することができる。端末100とサーバである電子金庫手段103は、無線によって通信する。なお、端末100は、ICカードリーダーを備えたパーソナルコンピュータ、またはセットトップボックス、または携帯型コ

ンピュータであっても良い。なお、端末１００と電子金庫手段１０３の間の通信は、有線通信であってもよい。なお、ＩＣカード５０１と同等の機能を持つものを、端末１００内に内蔵して構成してもよい。

電子財布手段１０１および電子情報登録手段１０６および電子情報復元手段１０７は、ソフトウェアと、このソフトウェア格納する記憶領域と、このソフトウェアを解釈して実行するためのＯＳおよびＣＰＵによって実現される。また、電子財布手段１０１は、電子財布記憶手段１０２の内容の参照と変更を行なうことができる。電子財布記憶手段１０２は、ＥＥＰＲＯＭなどの書き換え可能なメモリによって実現される。

電子価値情報とは電子現金や電子チケット、電子クーポンなどを表す電子情報であり、登録証とは前記電子価値情報を電子金庫手段１０３に登録したさいに発行される前記電子価値情報の控えを表す電子情報である。図３に電子財布記憶手段１０２での電子価値情報と登録証の管理方法を示す。電子財布手段１０１は、電子財布記憶手段１０２上にインデックス８５１を置く。前記インデックス８５１は、電子財布記憶手段１０２上に格納された情報に対するポイントと前記情報のサイズとポイントの先の情報の種別を表す記号の組をまとめたものである。これにより、電子財布手段１０１は次に示す機能を実現できる。

電子財布手段１０１は、電子財布記憶手段１０２中のインデックス８５１を参照してポイントとサイズを取得し、取得したポイントとサイズを用いて電子価値情報または登録証を取り出すことができる。電子財布手段１０１は、電子財布記憶手段１０２中のインデックス８５１を参照してすべてのポイントとサイズを取得し、それを用いて、すべての電子価値情報と登録証のタイトル情報を取得する。前記のポイントとサイズタイトルを用いて、全保管情報のリストを作成することができる。また、特定の条件に合致するポイントとサイズを取得することで、条件に合致する情報のリスト（例えば登録証のリストや有効期限完了まで残り一週間以内の情報のリストなど）を作成することもできる。

また、電子財布手段１０１は、電子財布記憶手段１０２中の空き領域に電子価値情報または登録証を書き込み、それに対応する種別とポイントとサイズの組の

エントリをインデックス 8 5 1 に追加することで、電子財布記憶手段 1 0 2 に電子価値情報または登録証を保管することができる。その逆に、インデックス 8 5 1 中に示されたポイントとサイズを参照して、前記ポイントとサイズが指す領域を消去し、前記ポイントとサイズに対応したエントリをインデックス 8 5 1 から削除することで、電子財布記憶手段 1 0 2 から電子価値情報または登録証を削除することができる。また、新規登録と削除を組み合わせることで、電子価値情報または登録証の情報を修正することができる。なお、上記の仕組みは、ＩＣカード 5 0 1 上のオペレーティングシステム（ＯＳ）が持つファイルシステムの機能を用いて実現しても良い。

電子情報登録手段 1 0 6 は、ソフトウェアと、このソフトウェアを格納する記憶領域と、このソフトウェアを解釈して実行するためのＯＳおよびＣＰＵによって構成される。なお、電子情報登録手段 1 0 6 と電子財布手段 1 0 1 はＯＳとＣＰＵを共有してもよい。電子情報登録手段 1 0 6 は、電子財布手段 1 0 1 から電子価値情報を取得することと、登録証を電子財布手段 1 0 1 に登録することを行う。また、電子情報登録手段 1 0 6 は、電子財布手段 1 0 1 から電子価値情報の一覧を取得する。

電子情報復元手段 1 0 7 は、ソフトウェアと、このソフトウェアを格納する記憶領域と、このソフトウェアを解釈して実行するためのＯＳおよびＣＰＵによって構成される。なお、電子情報復元手段 1 0 7 と電子財布手段 1 0 1 はＯＳとＣＰＵを共有してもよい。電子情報復元手段 1 0 7 は、電子財布手段 1 0 1 から登録証を取得することと、電子価値情報を電子財布手段 1 0 1 に登録することを行う。また、電子情報復元手段 1 0 7 は、電子財布手段 1 0 1 から登録証の一覧を取得する。

電子金庫手段 1 0 3 は、ワークステーションまたはパーソナルコンピュータなどのコンピュータ装置と、前記コンピュータシステム上で動作するソフトウェアから構成される。電子金庫手段 1 0 3 は、電子金庫記憶手段 1 1 0 の内容の参照と変更を行なうことができる。電子金庫記憶手段 1 1 0 は、電子金庫手段 1 0 3 が内容の参照と変更を行なうことができる記憶装置であり、ハードディスクなど

で実現される。電子金庫記憶手段 110 上には、前記コンピュータシステムの OS が管理するファイルシステムが構築されている。

図 2 (a) は電子価値情報の一例として電子価値情報 201 を示す。電子金庫手段 103 が電子価値情報 201 の登録要求を受けた場合、図 2 (c) に示す登録証 301 を電子価値情報 201 を用いて生成する。登録証 301 を生成する処理の流れを以下に説明する。

電子金庫手段 103 は、設定に基づいて、電子価値情報 201 から図 2 (b) に示すダイジェスト 302 を生成する。また、電子価値情報 201 を一方向性のハッシュ関数に通して X1 という数を生成する。電子金庫手段 103 が持つカウンタを参照し Y1 という数を取得する。前記カウンタは参照の度に 1 ずつ昇順で増加し、上限に達すれば 0 に戻るものであるとする。これらダイジェスト 302 とハッシュ値 X1 とカウンタ値 Y1 を組として登録証 301 とする。前記 X1 を生成するために用いたハッシュ関数として、MD5 や SHA1 などの分散性の高いものを用いることとする。なお、ダイジェスト 302 は空情報であってもよい。

図 4 は電子金庫手段 103 が電子金庫記憶手段 110 上に情報を保管する方法を示す。電子金庫手段 103 は、電子価値情報 201 をファイル 801、登録証 301 をファイル 802 として電子金庫手段 110 に保管する。登録証 301 の構成要素であるハッシュ値 X1 とカウンタ値 Y1 とファイル 801 のパス情報とファイル 802 のパス情報を組として、インデックスファイル 852 の 1 つのエントリとして登録する。インデックスファイル 852 は 1 エントリ 1 行の CSV ファイルであり、各行はカウンタ値によって昇順にソートされている。端末 100 から電子金庫手段 103 に登録証が提示された場合に、電子金庫手段 103 は電子金庫記憶手段 110 中のインデックスファイル 852 から登録証に対応する電子価値情報をカウンタ値の一致するエントリ群を検索し、その中からハッシュ値が一致するエントリ群にさらに絞り込み、登録証が完全に一致するエントリを抽出する。これにより登録証に対応する電子価値情報を高速に検索することが可能である。

ユーザが端末 100 を操作して電子価値情報 201 をバックアップする手順を、

以上に示した各手段を用いて示す。以下の手順での動作は、端末100にICカード501を装着した状態ですべてユーザによって行なわれる。

(1-1) 端末100が、電子情報登録手段106に電子価値情報リストを要求する。

(1-2) 電子情報登録手段106が、電子財布手段101に電子価値情報リストを要求する。

(1-3) 電子財布手段101が、電子価値情報のリストを生成し電子情報登録手段106に送る。

(1-4) 電子情報登録手段106が、前記電子価値情報リストを端末100に送る。

(1-5) 端末100が、前記電子価値情報リストから選択した電子価値情報201を電子情報登録手段106に要求する。

(1-6) 電子情報登録手段106が、電子財布手段101に電子価値情報201を要求する。

(1-7) 電子財布手段101が、電子価値情報201を電子財布記憶手段102から取得し、電子情報登録手段106に送る。

(1-8) 電子情報登録手段106が、電子価値情報201を端末100に送る。

(1-9) 端末100が、電子価値情報201の登録を電子金庫手段103に送る。

(1-10) 電子金庫手段103が、電子価値情報201を電子金庫記憶手段110に保管する。

(1-11) 電子金庫手段103が、登録証301を端末100に送る。

(1-12) 端末100が、登録証301を電子情報登録手段106に送る。

(1-13) 電子情報登録手段106が、登録証301の登録を電子財布手段101に要求する。

(1-14) 電子財布手段101が、電子価値情報201の内容と登録証301のダイジェスト302とを、電子価値情報201をハッシュ演算した値と登録証301のハッシュ値X1とを、それぞれ照合し、一致した場合に、登録証301を電子財布記憶手段102に保管し、完了通知を電子情報登録手段106に送る。一致しなかった場合はエラー通知を送る。

(1-15) 電子情報登録手段106が、電子財布手段101から取得した完了通知

またはエラー通知を端末 1 0 0 に送る。

なお、登録証 3 0 1 が正常に電子財布記憶手段 1 0 2 に保管された場合、電子財布記憶手段 1 0 2 上から電子価値情報 2 0 1 を削除してもよい。ＩＣカードのように記憶容量が少ないデバイスを用いる場合、これは記憶容量を効率的に利用する有効な手段である。

次に、ユーザが端末 1 0 0 を操作して電子財布記憶手段 1 0 2 に保管された登録証 3 0 1 に対応する電子価値情報 2 0 1 を電子財布記憶手段 1 0 2 上に復元する手順を示す。

(2-1) 端末 1 0 0 が、電子情報復元手段 1 0 7 に登録証リストを要求する。

(2-2) 電子情報復元手段 1 0 7 が、電子財布手段 1 0 1 に登録証リストを要求する。

(2-3) 電子財布手段 1 0 1 が、登録証のリストを生成し電子情報復元手段 1 0 7 に送る。(2-4) 電子情報復元手段 1 0 7 が、前記登録証リストを端末 1 0 0 に送る。

(2-5) 端末 1 0 0 が、前記登録証リストから選択した登録証 3 0 1 を電子情報復元手段 1 0 7 に要求する。

(2-6) 電子情報復元手段 1 0 7 が、電子財布手段 1 0 1 に登録証 3 0 1 を要求する。

(2-7) 電子財布手段 1 0 1 が、登録証 3 0 1 を電子財布記憶手段 1 0 2 から取得し、電子情報復元手段 1 0 7 に送る。

(2-8) 電子情報復元手段 1 0 7 が、登録証 3 0 1 を端末 1 0 0 に送る。

(2-9) 端末 1 0 0 が、電子金庫手段 1 0 3 に登録証 3 0 1 を提示し、対応する電子価値情報の取得を要求する。

(2-10) 電子金庫手段 1 0 3 は登録証 3 0 1 を用いて電子価値情報 2 0 1 を検索して取得し、端末 1 0 0 に送る。この時、電子金庫手段 1 0 3 は、検索した電子価値情報の内容と登録証 3 0 1 とを照合し、不整合であった場合には、電子価値情報 2 0 1 の復元処理を中止する。

(2-11) 端末 1 0 0 が、電子価値情報 2 0 1 を電子情報復元手段 1 0 7 に送る。

(2-12) 電子情報復元手段 1 0 7 が、電子価値情報 2 0 1 の登録を電子財布手段 1 0 1 に要求する。

(2-13) 電子財布手段 1 0 1 が、電子価値情報 2 0 1 を電子財布記憶手段 1 0 2 条に登録する。

(2-14) 電子情報復元手段 1 0 7 が、完了通知を端末 1 0 0 に送る。

以上説明したように、本実施例 1 の電子情報バックアップシステムによれば、ユーザが持つ電子価値情報を電子金庫記憶手段上にバックアップすることと、バックアップした電子価値情報の概要を電子金庫手段に問い合わせることなく認識できることと、必要に応じて電子価値情報を電子財布記憶手段上に復元することが可能となる。

実施例 2

次に、図 5、図 6、図 7、図 8、図 9 を用いて、本発明の請求項 4、5 に係る第 2 の実施例について説明する。図 5 は本実施例 2 における電子情報バックアップシステムの一例を示した構成図であり、本システムは実施例 1（図 1）で示されたシステムの端末 1 0 0 を端末 1 1 2 に置き換え、電子金庫手段 1 0 3 を電子金庫手段 1 1 3 に置き換え、IC カード 5 0 1 を IC カード 5 0 2 と置き換えたものである。IC カード 5 0 2 は、IC カード 5 0 1 に対して暗復号化手段 1 0 5 と鍵保管手段 1 0 4 と鍵管理手段 1 1 5 を追加し、電子情報登録手段 1 0 6 を電子情報登録手段 1 2 0 に変更し、電子情報復元手段 1 0 7 を電子情報復元手段 1 2 1 に変更したものである。

暗復号化手段 1 0 5 は、ソフトウェアと、このソフトウェアを格納する記憶領域と、このソフトウェアを解釈して実行するための OS および CPU によって構成される。鍵保管手段 1 0 4 は、EEPROM などの書き換え可能なメモリによって実現される。なお、暗復号化手段 1 0 5 と電子財布手段 1 0 1 は、OS と CPU を共有してもよい。また、鍵保管手段 1 0 4 と電子財布記憶手段 1 0 2 は、EEPROM を共有してもよい。

鍵保管手段 1 0 4 は、図 7 に示すように暗号鍵 4 0 1 と復号鍵 4 0 2 を保持する。本実施例 2 では、鍵保管手段 1 0 4 に保管された暗号鍵 4 0 1 と復号鍵 4 0

2のペアは、暗復号化手段105が生成する。暗復号化手段105は、公開鍵暗号方式を用いることとし、暗号鍵401を公開鍵、復号鍵402を秘密鍵とする。なお、暗復号化手段105の暗号化方式として共通鍵暗号方式を用いてもよい。その場合、暗号鍵401と復号鍵402は同一の鍵となる。鍵管理手段115は、鍵保管手段104に保管された鍵を取得する機能と、鍵保管手段104に新しい鍵を登録する機能と、鍵保管手段104から既存の鍵を削除する機能を持つ。

暗復号化手段105は、鍵管理手段115を通じて鍵保管手段104から暗号鍵401を取得し、入力された電子情報を前記暗号鍵401で暗号化した暗号化電子情報を返す機能と、鍵管理手段115を通じて鍵保管手段104から復号鍵402を取得し、入力された前記暗号化電子情報を前記復号鍵402で復号化して前記電子情報を返す機能と、入力情報に対するハッシュ値を暗号鍵401を用いて暗号化した情報（電子署名）を生成する機能を持つ。また逆に、復号鍵402を用いて前記電子署名を検証する機能も持つ。なお、暗号鍵401と復号鍵402は、ICカード502固有の共通鍵暗号方式の暗号鍵であってもよい。また、暗号鍵401と復号鍵402はそれぞれ、ICカード502固有の公開鍵暗号方式の公開鍵と秘密鍵の一对の鍵ペアであってもよい。

電子情報登録手段120は、実施例1の電子情報登録手段106が持つ機能をすべて持つと同時に、図6(a)に示すような登録電子価値情報203を生成する機能を持つ。電子情報登録手段120は、暗復号化手段105を用いて電子価値情報201から暗号化電子価値情報202を取得し、電子価値情報201から抽出した情報を用いてダイジェスト302を生成し、このダイジェスト302と、暗号化電子価値情報202と、暗復号化手段105を用いてダイジェスト302と暗号化電子価値情報202をまとめた情報から生成した署名303とを、合成して登録電子価値情報203を生成する。また、電子情報登録手段120は、鍵管理手段115を通じて鍵保管手段104から鍵情報を取得する機能を持つ。

電子情報復元手段121は、電子情報復元手段107の持つ機能をすべて持つと同時に、登録電子価値情報203内の署名303を暗復号化手段105を用いて検証して正当性を確認した後、登録電子価値情報203から暗号化電子価値情

報 2 0 2 を抽出して、暗復号化手段 1 0 5 を用いて電子価値情報 2 0 2 から電子価値情報 2 0 1 を復号する機能を持つ。また、電子情報復元手段 1 2 1 は、鍵管理手段 1 1 5 を通じて鍵情報を鍵保管手段 1 0 4 に登録する機能を持つ。

電子金庫手段 1 1 3 は、図 1 の電子金庫手段 1 0 3 のソフトウェアを変更したものであり、電子金庫手段 1 1 3 は、電子金庫記憶手段 1 1 0 の内容の参照と変更を行なうことができる。電子金庫手段 1 1 3 が登録電子価値情報 2 0 3 の登録要求を受けた場合、図 6 (b) に示す登録証 3 0 4 を登録電子価値情報 2 0 3 を用いて生成する。登録証 3 0 4 を生成する処理の流れを以下に説明する。

電子金庫手段 1 1 3 は、登録電子価値情報 2 0 3 からダイジェスト 3 0 2 を抽出する。また、暗号化電子価値情報 2 0 2 を一方向性のハッシュ関数に通して X 2 という数を生成する。電子金庫手段 1 1 3 が持つカウンタを参照し Y 2 という数を取得する。前記カウンタは参照の度に 1 ずつ昇順で増加し、上限に達すれば 0 に戻るものであるとする。これらダイジェスト 3 0 2 とハッシュ値 X 2 とカウンタ値 Y 2 を組として登録証 3 0 4 とする。前記 X 2 を生成するために用いたハッシュ関数として、MD 5 や SHA 1 などの分散性の高いものを用いることとする。登録証 3 0 4 はダイジェスト 3 0 2 の情報を含むため、それを参照することで登録された電子価値情報の概要を把握することができる。なお、ダイジェスト 3 0 2 は空情報の場合であってもよいが、その場合は登録証 3 0 4 から電子価値情報の概要を知ることはできない。

また、電子金庫手段 1 1 3 が復号鍵 4 0 2 の登録要求を受けた場合、図 8 (a) に示す登録証 3 0 5 を生成する。登録証 3 0 5 は、鍵情報に対する登録証であることを示すダイジェスト 3 0 6 と、復号鍵 4 0 2 から生成したハッシュ値 X 3 と、電子金庫手段 1 1 3 が持つカウンタ値 Y 3 とから構成される。ダイジェスト 3 0 6 は、図 8 (b) に示すように、鍵情報に対する登録証であることを示す情報種別と鍵情報とからなる。

電子価値情報に対する登録証 3 0 4 と、鍵情報に対する登録証 3 0 5 との区別は、電子価値情報に対する登録証 3 0 4 に含まれる情報種別と鍵情報に対応する登録証 3 0 5 に含まれる情報種別の違いによって行う。これにより、電子金庫手

段113が電子価値情報と鍵情報を電子金庫記憶手段110に格納する際に、両者に対して同じ管理方法を用いることができる。図9はその管理方法を示した図である。

電子金庫手段113は、実施例1における電子金庫手段103の機能をすべて持つと同時に、登録電子価値情報203をファイル803、登録証304をファイル804、復号鍵402をファイル805、登録証305をファイル806として、それぞれ電子金庫記憶手段110に保管する。登録証304の構成要素であるハッシュ値X2とカウンタ値Y2とファイル803のパス情報とファイル804のパス情報を組として、インデックスファイル853の1つのエントリとして登録する。また、登録証305の構成要素であるハッシュ値X3とカウンタ値Y3とファイル805のパス情報とファイル806のパス情報を組として、インデックスファイル853の1つのエントリとして登録する。インデックスファイル853は1エントリ1行のCSVファイルであり、各行はカウンタ値によって昇順にソートされている。端末112から電子金庫手段113に登録証が提示された場合に、電子金庫手段113は、電子金庫記憶手段110中のインデックスファイル853から登録証に対応する電子価値情報をカウンタ値の一致するエントリ群を検索し、その中からハッシュ値が一致するエントリ群にさらに絞り込み、登録証が完全に一致するエントリを抽出する。これにより登録証に対応する電子価値情報を高速に検索することが可能である。なお、電子価値情報と鍵情報のインデックスファイルを分けても良い。

次に、ユーザが端末112を操作して電子価値情報201をバックアップする手順を示す。以下の手順での選択動作はすべてユーザによって行なわれる。

- (1-1) 端末112が、電子情報登録手段120に電子価値情報リストを要求する。
- (1-2) 電子情報登録手段120が、電子財布手段101に電子価値情報リストを要求する。
- (1-3) 電子財布手段101が、電子価値情報のリストを生成し電子情報登録手段120に送る。
- (1-4) 電子情報登録手段120が、前記電子価値情報リストを端末112に送る。

(1-5) 端末 1 1 2 が、前記電子価値情報リストから選択した電子価値情報 2 0 1 の選択を電子情報登録手段 1 2 0 に通知する。

(1-6) 電子情報登録手段 1 2 0 が、電子財布手段 1 0 1 に電子価値情報 2 0 1 を要求する。

(1-7) 電子財布手段 1 0 1 が、電子価値情報 2 0 1 を電子財布記憶手段 1 0 2 から取得し、電子情報登録手段 1 2 0 に送る。

(1-8) 電子情報登録手段 1 2 0 が、暗復号化手段 1 0 5 を用いて電子価値情報 2 0 1 から暗号化電子価値情報 2 0 2 を取得し、電子価値情報 2 0 1 と暗号化電子価値情報 2 0 2 から登録電子価値情報 2 0 3 を生成する。

(1-9) 電子情報登録手段 1 2 0 が、登録電子価値情報 2 0 3 を端末 1 1 2 に送る。

(1-10) 端末 1 1 2 が、登録電子価値情報 2 0 3 の登録を電子金庫手段 1 1 3 に要求する。

(1-11) 電子金庫手段 1 1 3 が、登録電子価値情報 2 0 3 を電子金庫記憶手段 1 1 0 に保管すると同時に、登録電子価値情報 2 0 3 から登録証 3 0 4 を生成する。

(1-12) 電子金庫手段 1 1 3 が、登録証 3 0 4 を端末 1 0 0 に送る。

(1-13) 端末 1 1 2 が、登録証 3 0 4 を電子情報登録手段 1 2 0 に送る。

(1-14) 電子情報登録手段 1 2 0 が、登録証 3 0 4 の登録を電子財布手段 1 0 1 に要求する。

(1-15) 電子財布手段 1 0 1 が、電子価値情報 2 0 1 の内容から生成したダイジェストと登録証 3 0 4 のダイジェスト 3 0 2 とを、前記ダイジェストをハッシュ演算した値と登録証 3 0 4 のハッシュ値 X 2 とを、それぞれ照合し、一致した場合に、登録証 3 0 4 を電子財布記憶手段 1 0 2 に保管し、完了通知を電子情報登録手段 1 2 0 に送る。一致しなかった場合はエラー通知を送る。

(1-16) 電子情報登録手段 1 2 0 が、電子財布手段 1 0 1 から取得した完了通知またはエラー通知を端末 1 1 2 に送る。

次に、ユーザが端末 1 1 2 を操作して電子財布記憶手段 1 0 2 に保管された登録証 3 0 4 に対応する電子価値情報 2 0 1 を電子財布記憶手段 1 0 2 上に復元する手順を示す。

- (2-1) 端末 1 1 2 が、電子情報復元手段 1 2 1 に登録証リストを要求する。
- (2-2) 電子情報復元手段 1 2 1 が、電子財布手段 1 0 1 に登録証リストを要求する。
- (2-3) 電子財布手段 1 0 1 が、登録証のリストを生成し電子情報復元手段 1 2 1 に送る。(2-4) 電子情報復元手段 1 2 1 が、前記登録証リストを端末 1 1 2 に送る。
- (2-5) 端末 1 1 2 が、前記登録証リストから選択した登録証 3 0 4 を電子情報復元手段 1 2 1 に要求する。
- (2-6) 電子情報復元手段 1 2 1 が、電子財布手段 1 0 1 に登録証 3 0 4 を要求する。
- (2-7) 電子財布手段 1 0 1 が、登録証 3 0 4 を電子財布記憶手段 1 0 2 から取得し、電子情報復元手段 1 2 1 に送る。
- (2-8) 電子情報復元手段 1 2 1 が、登録証 3 0 4 を端末 1 1 2 に送る。
- (2-9) 端末 1 1 2 が、電子金庫手段 1 1 3 に登録証 3 0 4 を提示し、対応する電子価値情報の取得を要求する。
- (2-10) 電子金庫手段 1 0 3 は登録証 3 0 4 を用いて登録電子価値情報 2 0 3 を検索して取得し、端末 1 1 2 に送る。この時、電子金庫手段 1 0 3 は、検索した電子価値情報の内容と登録証 3 0 4 とを照合し、不整合であった場合には、電子価値情報 2 0 1 の復元処理を中止する。
- (2-11) 端末 1 1 2 が、登録電子価値情報 2 0 3 を電子情報復元手段 1 2 1 に送る。
- (2-12) 電子情報復元手段 1 2 1 が、暗復号化手段 1 0 5 を用いて登録電子価値情報 2 0 3 の署名 3 0 3 を検証し、成功したとき、登録電子価値情報 2 0 3 から抽出した暗号化電子価値情報 2 0 2 を暗復号化手段 1 0 5 を用いて復号化して電子価値情報 2 0 1 を取得する。
- (2-13) 電子情報復元手段 1 2 1 が、電子価値情報 2 0 1 の登録を電子財布手段 1 0 1 に要求する。
- (2-14) 電子財布手段 1 0 1 が電子価値情報 2 0 1 を電子財布記憶手段 1 0 2 に

登録する。

(2-15) 電子情報復元手段121が、完了通知を端末112に送る。

また、ユーザが端末112を操作して復号鍵402をバックアップする手順を次に示す。以下の手順での選択動作はすべてユーザによって行なわれる。

(3-1) 端末112が、復号鍵402を電子情報登録手段120に要求する。

(3-2) 電子情報登録手段120が、鍵管理手段115に復号鍵402を要求する。

(3-3) 鍵管理手段115が、復号鍵402を鍵保管手段104から取得し、電子情報登録手段120に送る。

(3-4) 電子情報登録手段120が、復号鍵402を端末112に送る。

(3-5) 端末112が、復号鍵402を電子金庫手段113に登録を要求する。

(3-6) 電子金庫手段113が、復号鍵402を電子金庫記憶手段110に保管すると同時に、登録証305を生成する。

(3-7) 電子金庫手段113が、登録証305を端末112に送る。

(3-8) 端末112が、登録証305を電子情報登録手段120に送る。

(3-9) 電子情報登録手段120が、登録証305の登録を電子財布手段101に要求する。

(3-10) 電子財布手段101が、登録証305を電子財布記憶手段102に保管し、完了通知を電子情報登録手段120に送る。

(3-11) 電子情報登録手段120が、電子財布手段101から取得した完了通知またはエラー通知を端末112に送る。

次に、ユーザが端末112を操作して電子財布記憶手段102に保管された登録証305に対応する復号鍵402を鍵保管手段104上に復元する手順を示す。

(4-1) 端末112が、電子情報復元手段121に登録証リストを要求する。

(4-2) 電子情報復元手段121が、電子財布手段101に登録証リストを要求する。

(4-3) 電子財布手段101が、登録証のリストを生成して電子情報復元手段121に送る。

(4-4) 電子情報復元手段121が、前記登録証リストを端末112に送る。

(4-5) 端末 1 1 2 が、前記登録証リストから選択した登録証 3 0 5 を電子情報復元手段 1 2 1 に要求する。

(4-6) 電子情報復元手段 1 2 1 が、電子財布手段 1 0 1 に登録証 3 0 5 を要求する。

(4-7) 電子財布手段 1 0 1 が、登録証 3 0 5 を電子財布記憶手段 1 0 2 から取得し、電子情報復元手段 1 2 1 に送る。

(4-8) 電子情報復元手段 1 2 1 が、登録証 3 0 5 を端末 1 1 2 に送る。

(4-9) 端末 1 1 2 が、電子金庫手段 1 1 3 に登録証 3 0 5 を提示し、対応する復号鍵の取得を要求する。

(4-10) 電子金庫手段 1 0 3 は登録証 3 0 5 を用いて復号鍵 4 0 2 を検索して取得し、端末 1 1 2 に送る。

(4-11) 端末 1 1 2 が、復号鍵 4 0 2 を電子情報復元手段 1 2 1 に送る。

(4-12) 電子情報復元手段 1 2 1 が、復号鍵 4 0 2 の登録を鍵管理手段 1 1 5 に要求する。

(4-13) 鍵管理手段 1 1 5 が復号鍵 4 0 2 を鍵保管手段 1 0 4 に登録する。

(4-14) 電子情報復元手段 1 2 1 が、完了通知を端末 1 1 2 に送る。

なお、電子情報登録手段 1 2 0 と電子金庫手段 1 1 3 の通信は、端末 1 1 2 を含めた通信路での盗聴を防ぐために、暗号化通信を行ってもよい。この場合、端末 1 1 2 も通信されている情報の内容を知ることができない。また、電子情報復元手段 1 2 1 と電子金庫手段 1 1 3 の通信は、端末 1 1 2 を含めた通信路での盗聴を防ぐために、暗号化通信を行ってもよい。この場合、端末 1 1 2 も通信されている情報の内容を知ることができない。

以上説明したように、本実施例 2 の電子情報バックアップシステムによれば、ユーザが持つ電子価値情報を電子金庫手段には秘密の鍵を用いて暗号化してバックアップすることと、バックアップした電子価値情報の概要をローカルで把握することと、必要に応じて暗号化してバックアップした電子価値情報を電子金庫手段から復元することと、復号鍵を電子金庫手段に保管することで、鍵保管手段が壊れた場合にも電子価値情報を復元することが可能になる。

実施例 3

次に、図 10 を用いて本発明の請求項 6 に係る第 3 の実施例について説明する。図 10 は本実施例 3 における電子情報バックアップシステムの一例を示した構成図であり、本システムは実施例 2（図 5）で示されたシステムの端末 112 を端末 114 に置き換え、端末 114 と通信する電子金庫手段 123 と、電子金庫手段 123 の記憶装置である電子金庫記憶手段 122 を追加したものである。電子金庫手段 123 と電子金庫記憶手段 122 は、電子金庫手段 113 と電子金庫記憶手段 110 と同等の機能を持つ。端末 114 は、端末 112 が持つ機能をすべて持つと同時に、電子金庫手段 123 に対しても電子価値情報および復号鍵のバックアップ先とする機能を持つ。

本実施例 3 では、電子金庫手段 113 に対して電子価値情報 201 から生成される登録電子価値情報 203 のバックアップを行い、電子金庫手段 123 に対して復号鍵 402 のバックアップを行うこととする。復号鍵 402 のバックアップ手順は、バックアップ先を電子金庫手段 113 から電子金庫手段 123 に変更したことを除いて、実施例 2 と同じ方式を用いることとする。このため、電子金庫手段 113 と電子金庫手段 123 が共謀することがない限り、電子金庫手段 113 と電子金庫手段 123 には電子価値情報 201 を解読されない。

なお、電子情報登録手段 120 と電子金庫手段 113 の通信は、端末 114 を含めた通信路での盗聴を防ぐために、暗号化通信を行ってもよい。この場合、端末 114 も通信されている情報の内容を知ることができない。また、電子情報復元手段 121 と電子金庫手段 113 の通信は、端末 114 を含めた通信路での盗聴を防ぐために、暗号化通信を行ってもよい。この場合、端末 114 も通信されている情報の内容を知ることができない。

さらに、電子情報登録手段 120 と電子金庫手段 123 の通信は、端末 114 を含めた通信路での盗聴を防ぐために、暗号化通信を行ってもよい。この場合、端末 114 も通信されている情報の内容を知ることができない。また、電子情報復元手段 121 と電子金庫手段 123 の通信は、端末 114 を含めた通信路での盗聴を防ぐために、暗号化通信を行ってもよい。この場合、端末 114 も通信さ

れている情報の内容を知ることはできない。

以上説明したように、本実施例 3 の電子情報バックアップシステムによれば、ユーザが持つ電子価値情報を電子金庫手段には秘密の鍵を用いて暗号化してバックアップすることと、バックアップした電子価値情報の概要をローカルで把握することと、必要に応じて暗号化してバックアップした電子価値情報を電子金庫手段から復元することと、復号鍵を暗号化した電子価値情報と別の電子金庫手段に保管することで、二つの電子金庫手段が共謀しない限り元の電子価値情報を取得できないようにすることが可能となる。

実施例 4

次に、図 11 を用いて、本発明の請求項 7、8、9 に係る第 4 の実施例について説明する。図 11 は本実施例 4 における電子情報バックアップシステムの一例を示した構成図であり、本システムは実施例 3（図 10）で示されたシステムの端末 114 を端末 116 に置き換え、IC カード 502 を IC カード 503 と置き換えたものである。IC カード 503 は、IC カード 502 に対して電子情報分割手段 126 と電子情報合成手段 127 を追加し、電子情報登録手段 120 を電子情報登録手段 124 に変更し、電子情報復元手段 121 を電子情報復元手段 125 に変更したものである。電子情報分割手段 126 および電子情報合成手段 127 は、ソフトウェアと、このソフトウェアを格納する記憶領域と、このソフトウェアを解釈して実行するための OS および CPU によって構成される。

以下、本実施例 4 の動作について説明するが、基本的な動作は上記実施例 2 および 3 と同様であるので、以下には実施例 2 および 3 と異なる部分についてのみ説明する。電子情報分割手段 126 は、電子価値情報を元の電子価値情報へ復元するための識別子を付加した任意の数の部分電子情報に分割する。電子情報合成手段 127 は、この分割電子情報のすべてから元の電子価値情報を復元する。電子情報登録手段 124 は、電子価値情報の分割を電子情報分割手段 126 に要求して複数の部分電子情報を取得するとともに、その部分電子情報のすべてを電子金庫手段 113 に登録して同数の部分情報登録証を取得する。そして、電子情報復元手段 125 は、取得した部分情報登録証のすべてをそれぞれの部分情報登録

証に対応する電子金庫手段113に提示して同数の部分電子情報を取得し、電子情報合成手段127が、その取得した部分電子情報のすべてから電子価値情報を電子財布手段101上に復元する。

本実施例4では、電子情報登録手段124は、登録する分割電子情報を暗復号化手段105を用いて暗号化して暗号化分割電子情報を取得し、取得した暗号化分割電子情報を電子金庫手段113に登録して対応する登録証を取得するようにしているが、逆に、電子価値情報を暗復号化手段105を用いて暗号化して暗号化電子情報を取得し、取得した暗号化電子情報を電子情報分割手段126を用いて分割暗号化電子情報を取得するとともに、その分割暗号化電子情報を電子金庫113に登録して対応する登録証を取得するようにしてもよい。また、上記実施例3のように、電子金庫手段113に対しては暗号化分割電子情報のバックアップを行い、電子金庫手段123に対しては復号鍵のバックアップを行うようにしてもよい。

実施例5

次に、図12を用いて、本発明の請求項10に係る第5の実施例について説明する。図12は本実施例5における電子情報バックアップシステムの一例を示した構成図であり、本システムは実施例3（図10）で示されたシステムの端末114を端末117に置き換え、ICカード502をICカード504に置き換えたものである。ICカード504は、ICカード502に対して電子情報結合手段130と電子情報結合解除手段131を追加し、電子情報登録手段120を電子情報登録手段128に変更し、電子情報復元手段121を電子情報復元手段129に変更したものである。電子情報結合手段130は、複数の電子価値情報を結合して一つの結合電子情報として出力する。電子情報結合解除手段131は、結合電子情報を複数の元の電子情報に分離する。電子情報結合手段130および電子情報結合解除手段131は、ソフトウェアと、このソフトウェアを格納する記憶領域と、このソフトウェアを解釈して実行するためのOSおよびCPUによって構成される。

以下、本実施例5の動作について説明するが、基本的な動作は上記実施例3と

同様であるので、以下には実施例 3 と異なる部分についてのみ説明する。電子情報結合手段 1 3 0 は、複数の電子価値情報の組から 1 つの結合電子情報を生成し、電子情報登録手段 1 2 8 が、この結合電子情報を電子金庫手段 1 1 3 に登録して対応する結合電子情報登録証を取得し、電子情報復元手段 1 2 9 が、この結合電子情報登録証を提示して電子金庫手段 1 1 3 から対応する結合電子情報を取得し、電子情報結合解除手段 1 3 1 が、この結合電子情報から元の複数の電子価値情報の組を生成して電子財布手段 1 0 1 上に復元する。

本実施例 5 では、電子情報登録手段 1 2 8 は、登録する結合電子情報を暗復号化手段 1 0 5 を用いて暗号化して結合暗号化電子情報を取得し、取得した結合暗号化電子情報を電子金庫手段 1 1 3 に登録して対応する登録証を取得するようにしているが、逆に、複数の電子価値情報をそれぞれ暗復号化手段 1 0 5 を用いて暗号化して暗号化電子情報を取得し、取得した暗号化電子情報を電子情報結合手段 1 3 0 を用いて結合暗号化電子情報を電子金庫手段 1 1 3 に登録して対応する登録証を取得するようにしてもよい。また、上記実施例 3 のように、電子金庫手段 1 1 3 に対しては結合暗号化電子情報のバックアップを行い、電子金庫手段 1 2 3 に対しては復号鍵のバックアップを行うようにしてもよい。

実施例 6

次に、図 1 3 を用いて、本発明の請求項 1 1、1 2 に係る第 6 の実施例について説明する。図 1 3 は本実施例 6 における電子情報バックアップシステムの一例を示した構成図であり、本システムは実施例 4 (図 1 1) と実施例 5 (図 1 2) で示されたシステムを結合したものであり、新たな端末 1 1 8 と IC カード 5 0 5 を用いたものである。IC カード 5 0 5 は、電子情報登録手段 1 3 2 および電子情報復元手段 1 3 3 と、電子分割手段 1 3 4 および電子合成手段 1 3 5 と、電子情報結合手段 1 3 6 および電子情報結合解除手段 1 3 7 とを備えている。その他は実施例 4 および 5 と同じである。

以下、本実施例 6 の動作について説明するが、本実施例 6 が上記実施例 4、5 と異なるのは、本実施例 6 では、復号鍵を 2 つの部分鍵に分割するとともに、一方の部分鍵を電子価値情報と組にして一方の電子金庫手段 1 1 3 に登録し、他方

の部分鍵を他方の電子金庫手段123に登録することである。電子情報分割手段134は、電子情報登録手段132が鍵保管手段104から鍵管理手段105を通じて取得した復号鍵情報を複数の部分鍵に分割する。暗復号化手段105は、電子情報登録手段132が電子財布手段101から取得した電子価値情報を暗号化して暗号化電子情報を取得する。電子情報結合手段136は、これら暗号化電子情報と分割された部分鍵の一部である部分鍵群Aとを結合して結合電子情報を出力する。電子情報登録手段132は、この結合電子情報を電子金庫手段113に、残りの部分鍵である部分鍵群Bを別の電子金庫手段123に登録してそれぞれ対応する登録証を取得する。電子情報復元手段133は、それらの登録証を対応する電子金庫手段113および123に提示して結合電子情報と部分鍵群Bとを取得する。電子情報結合解除手段137は、その結合電子情報を暗号化電子情報と部分鍵群Aとに分離し、電子情報合成手段135は、部分鍵群Aと部分鍵群Bとを合成して復号鍵を生成し、暗復号化手段105は、暗号化電子情報を復号して電子価値情報を出力し、電子情報復元手段133は、その鍵情報を鍵管理手段115を通じて鍵保管手段104上に復元するとともに、電子価値情報を電子財布手段101上に復元する。

上記した説明は、電子価値情報を2つに分割した例であるが、3つ以上のさらに多くに分割してもよい。また、分割した電子価値情報を1つの電子金庫手段にのみ預けるようにしてもよい。また、分割した電子価値情報の全てを預ける必要は必ずしもなく、必要なものだけを預けるようにしてもよい。さらに、上記実施例4のように、電子価値情報自体を複数に分割して、一方の分割電子情報を一方の分割鍵情報と組み合わせて一方の電子金庫手段113に登録し、他方の分割電子情報を他方の分割鍵情報と組み合わせて他方の電子金庫手段123に登録するようにしてもよい。また、上記実施例5のように、電子価値情報として複数の電子価値情報を組み合わせた電子価値情報を使用するようにしてもよい。

以上に説明したシステムを用いることで、ユーザが持つ電子価値情報を電子金庫手段には秘密の鍵を用いて暗号化してバックアップすることと、バックアップした電子価値情報の概要をローカルで把握することと、必要に応じて暗号化して

バックアップした電子価値情報を電子金庫手段から復元することと、復号鍵を分割して、一方の分割鍵を電子価値情報とともに一方の電子金庫サーバにバックアップし、他方の分割鍵を他方の電子金庫サーバにバックアップすることで、復号鍵の一部を取得しただけでは、暗号化された電子価値情報を解読することはできないので、安全に鍵情報ひいては電子価値情報をバックアップすることが可能となる。

実施例 7

次に、図 14 を用いて、本発明の請求項 13 に係る第 7 の実施例について説明する。図 14 は本実施例 7 における電子情報バックアップシステムの一例を示した構成図であり、本システムは実施例 6（図 13）で示された IC カード 505 を IC カード 506 に置き換えたものである。IC カード 506 は、IC カード 505 に対して、鍵管理手段 138 の管理の基に、鍵保管手段 139 が、復号鍵を数学的に生成するために用いる元の暗号種（たね）情報 140 と、この暗号種情報から復号鍵を生成する復号鍵生成アルゴリズム 141 とを保持している。暗復号化手段 142 は、暗号種情報 140 に復号鍵生成アルゴリズム 141 をかけて復号鍵を生成する。暗号種情報 140 および復号鍵生成アルゴリズム 141 は、始めから鍵保管手段 139 に保持してもよく、またはどちらか一方を保持して、後から他方を外部からダウンロードしてもよく、両方とも外部からダウンロードしてもよい。暗号種情報としては、素数やその他の公知のものが使用可能であり、復号鍵だけでなく、暗号鍵と復号鍵の鍵ペアを数学的に生成する元となる情報としてもよい。

以下、本実施例 7 の動作について説明するが、基本的な動作は上記実施例 1 から 6 と同様であるので、以下にはこれらの実施例と異なる部分についてのみ説明する。

- (1-1) 端末 118 が、暗復号化手段 142 に対して復号鍵の取得を要求する。
- (1-2) 暗復号化手段 142 は、鍵管理手段 138 を通じて鍵保管手段 139 を参照し、暗号種情報 140 を取得する。
- (1-3) 暗復号化手段 142 は、暗号種情報 140 を電子情報登録手段 132 に渡

す。

(1-4) 電子情報登録手段132は、端末118を通じて電子金庫手段123に暗号種情報140の登録を要求する。

(1-5) 電子金庫手段123は、暗号種情報140を電子金庫記憶手段122に格納し、端末118に暗号種情報登録証を送付して登録完了を通知する。

(1-6) 端末118は、暗号種登録証を電子情報登録手段132に渡す。

(1-7) 鍵管理手段138は、暗号種登録証を鍵保管手段139に渡し、鍵保管手段139から暗号種情報140を削除する。

(2-1) 端末118が、電子財布手段101に電子価値情報リストを要求する。電子財布手段101は、電子価値情報のリストを生成し、端末118に送る。

(2-2) 端末118は、電子価値情報リストから選択した電子価値情報の提供を電子財布手段101に要求する。電子財布手段101は、電子価値情報を電子財布記憶手段102から取得する。暗号化手段142は、電子価値情報から暗号化電子価値情報を生成し、電子財布手段101に送る。電子財布手段101は、暗号化電子価値情報を電子登録手段132を通じて端末118に送る。

(2-3) 端末118は、暗号化電子価値情報の登録を電子金庫手段113に要求する。電子金庫手段113は、暗号化電子価値情報を電子金庫記憶手段110に保管するとともに、電子情報登録証を生成し、その登録証を端末118に送る。

(2-4) 端末118は、電子情報登録証の保管を電子情報登録手段132を通じて電子財布手段101に要求する。電子財布手段101は、電子情報登録証を電子財布記憶手段102に保管し、完了通知を端末118に送る。

(3-1) 端末118が、電子情報復元手段133を通じて暗復号化手段142に復号鍵を要求する。

(3-2) 鍵管理手段138は、鍵保管手段139から暗号種情報登録証を抽出して、暗復号化手段142に渡す。

(3-3) 暗復号化手段142は、暗号種情報登録証を電子情報復元手段133に渡し、端末118は、電子情報復元手段133を通じて、電子金庫手段123に暗号種情報登録証を提示して暗号種情報の返還を要求する。

(3-4) 電子金庫手段 1 2 3 は、暗号種情報登録証から該当する暗号種情報を電子金庫記憶手段 1 2 2 から取り出し、端末 1 1 8 に渡す。

(3-5) 暗復号化手段 1 4 2 は、鍵管理手段 1 3 8 を通じて鍵保管手段 1 3 9 から復号鍵生成アルゴリズム 1 4 1 を受け取るとともに、その復号鍵生成アルゴリズム 1 4 1 を、電子情報復元手段 1 3 3 を通じて受け取った暗号種情報にかけて復号鍵を生成する。

(3-6) 暗復号化手段 1 4 2 は、復元した復号鍵を鍵管理手段 1 3 8 を通じて鍵保管手段 1 3 9 に保管する。

(3-7) 暗復号化手段 1 4 2 は、復号鍵の復元が完了したことを端末 1 1 8 に通知する。

なお、本実施例 7 では、電子価値情報を電子金庫手段 1 1 3 に登録し、暗号種情報を電子金庫手段 1 2 3 に登録したが、両者を 1 つの電子金庫手段に登録してそれぞれについての登録証を受領するようにしてもよい。また、上記実施例 6 のように、暗号種情報を電子分割手段 1 3 4 により分割して、その一方を電子結合手段 1 3 6 により電子価値情報と組み合わせて電子金庫手段 1 1 3 に登録し、他方の分割種情報を他方の電子金庫手段 1 2 3 に登録し、復元時には、電子金庫手段 1 1 3 から受け取った電子価値情報を電子結合解除手段 1 3 7 により電子価値情報と一方の種情報とに分離し、この分離した種情報と、電子金庫手段 1 2 3 から受け取った他方の種情報を電子情報結合手段 1 3 5 により結合して 1 つの種情報としてもよい。

以上に説明したシステムを用いることで、ユーザが持つ電子価値情報を電子金庫手段には秘密の鍵を用いて暗号化してバックアップすることと、バックアップした電子価値情報の概要をローカルで把握することと、必要に応じて暗号化してバックアップした電子価値情報を電子金庫手段から復元することと、暗号化を解読する復号鍵そのものをバックアップするのではなく、その元となる暗号種情報をバックアップすることで、暗号種情報を取得しただけでは復号することができないので、極めて安全に鍵情報ひいては電子価値情報をバックアップすることが可能となる。

実施例 8

次に、図 15 を用いて、本発明の請求項 14 に係る第 8 の実施例について説明する。図 15 は本実施例 7 における電子情報バックアップシステムの一例を示した構成図であり、本システムは実施例 6（図 13）で示されたシステムの端末 118 を端末 119 に置き換え、IC カード 505 を IC カード 507 と置き換えたものである。IC カード 507 は、IC カード 505 に対して電子情報登録手段 132 を電子情報登録手段 143 に変更し、電子情報復元手段 133 を電子情報復元手段 144 に変更したものである。端末 119 には、所有者情報入力手段 145 と所有者認証情報入力手段 146 が接続されている。

以下、本実施例 8 の動作について説明するが、基本的な動作は上記実施例 1 から 6 と同様であるので、以下にはこれらの実施例と異なる部分についてのみ説明する。端末 119 には、所有者情報入力手段 145 から所有者固有の所有者情報を入力するとともに、所有者認証情報入力手段 146 から所有者情報に対応する所有者認証情報を入力する。電子情報登録手段 143 は、電子価値情報と所有者認証情報入力手段 146 より取得した所有者認証情報とを組として電子金庫手段 113 に登録する。電子情報復元手段 144 は、所有者情報入力手段 145 より取得した所有者情報を電子金庫手段 113 に提示し、所有者認証情報との照合が成功した時に、電子価値情報を取得することができる。なお、所有者情報と所有者認証情報とは、同一の情報を用いて単純に比較することでもよく、所有者認証情報として所有者情報を一方向性関数で計算した値を用いてもよい。また、所有者情報としてパスワードを用いてもよく、また、指紋や掌紋、虹彩などの生体情報を用いてもよい。

以上に説明したシステムを用いることで、ユーザが持つ電子価値情報を電子金庫手段には秘密の鍵を用いて暗号化してバックアップすることと、バックアップした電子価値情報の概要をローカルで把握することと、必要に応じて暗号化してバックアップした電子価値情報を電子金庫手段から復元することと、前記の暗号化を解読する復号鍵を紛失した場合にも、認証が成功すればその鍵を鍵保管手段上に復元することで暗号化された電子価値情報を復号することと、安全な方法で

認証を実現することが可能となる。

実施例 9

次に、図 16 を用いて、本発明の請求項 15、16、17 に係る第 9 の実施例について説明する。図 16 は本実施例 9 における電子情報バックアップシステムの一例を示した構成図であり、本システムは実施例 8（図 15）で示されたシステムの端末 119 を端末 147 に置き換え、この端末 147 に、所有者情報入力手段 145 と所有者認証情報保管手段 148 と所有者認証手段 149 とを接続したものである。

以下、本実施例 9 の動作について説明するが、基本的な動作は上記実施例 1 から 6 と同様であるので、以下にはこれらの実施例と異なる部分についてのみ説明する。端末 147 には、所有者情報入力手段 145 から所有者固有の所有者情報が入力される。所有者認証情報保管手段 148 は、入力された所有者情報に対応する所有者認証情報が保持されている。所有者認証手段 149 は、入力された所有者情報と保管された所有者認証情報とを対照して正当性を検証する。検証の結果、正当な所有者と認証された場合は、端末 147 は、そのことを電子金庫手段 113 に通知し、電子金庫手段 113 は、電子情報登録手段 143 と電子金庫手段 113 との間の暗号化通信路を構築する。電子情報登録手段 143 は、この暗号化通信路を通して電子価値情報を電子金庫手段 113 に登録し、電子金庫手段 113 は、認証結果に対応する所有者認証情報と電子価値情報とを組として電子金庫記憶手段 110 に保持する。これにより、電子情報復元手段 144 は、上記の暗号化通信路を通して認証結果に基づく所有者認証情報に対応した電子価値情報を取得することができる。

なお、所有者情報入力手段 145 と所有者認証手段 149 が一時的に利用する共通鍵を生成して共有し、この共通鍵によって所有者情報を暗号化して所有者認証手段 149 に送信するようにしてもよい。また、所有者情報入力手段 145 が、所有者認証手段 149 固有の秘密鍵に対応した公開鍵で所有者情報を暗号化し、この暗号化した所有者情報を所有者認証手段 149 に送信するようにしてもよい。

また、所有者情報と所有者認証情報とは、同一の情報を用いて単純に比較する

ようにしてもよく、所有者認証情報として所有者情報を一方向性関数で計算した値を用いてもよい。また、所有者情報としてパスワードを用いてもよく、指紋や掌紋、虹彩などの生体情報を用いてもよい。

実施例 10

次に、図 17 を用いて、本発明の請求項 18、19 に係る第 10 の実施例について説明する。図 17 は本実施例 10 における電子情報バックアップシステムの一例を示した構成図であり、本システムは実施例 8 (図 15) で示されたシステムの端末 119 を端末 150 に置き換え、この端末 150 に認証機器読み取り手段 151 を接続するとともに、電子金庫手段 113 を電子金庫手段 152 に置き換えたものである。認証機器読み取り手段 151 は、認証機器としての IC カードを読み取るための IC カードリーダである。また、電子金庫手段 152 には、認証確認情報保管手段 153 からの情報を基に、認証機器としての IC カードの正当性を検証するための認証確認手段 154 が接続されている。

以下、本実施例 10 の動作について説明するが、基本的な動作は上記実施例 1 から 6 と同様であるので、以下にはこれらの実施例と異なる部分についてのみ説明する。端末 150 には、認証機器読み取り手段 151 が読み取った認証機器としての IC カードの ID 情報が入力される。端末 150 は、この ID 情報を電子金庫手段 152 に送る。電子金庫手段 152 は、その ID 情報を認証確認手段 154 に送ると、認証確認手段 154 は、認証確認情報保管手段 153 から対応する ID 情報を読み出して対照して正当性を検証する。検証の結果、正当な所有者と認証された場合は、電子金庫手段 152 は、その情報を端末 150 に送り、電子情報登録手段 143 と電子金庫手段 152 との間の暗号化通信路を構築するとともに、この暗号化通信路を通して電子情報登録手段 143 が電子価値情報を電子金庫手段 152 に登録する。電子金庫手段 152 は、認証結果に対応する所有者認証情報と電子価値情報とを組として電子金庫記憶手段 110 に保持する。これにより、電子情報復元手段 144 は、上記の暗号化通信路を通して認証結果に基づく所有者認証情報に対応した電子価値情報を取得することができる。

なお、本実施例 10 では、認証機器として IC カードを用い、認証機器読み取

り手段としてＩＣカードリーダを用いているが、セキュリティ機能を有するメモリカードとメモリカードリーダを用いてもよい。

実施例 1 1

次に、図 1 8 を用いて、本発明の請求項 2 0、2 1 に係る第 1 1 の実施例について説明する。図 1 8 は本実施例 1 1 における電子情報バックアップシステムの一例を示した構成図であり、本システムは実施例 8（図 1 5）で示されたシステムの端末 1 1 9 を端末 1 6 0 に置き換え、ＩＣカード 5 0 7 をＩＣカード 5 0 8 に置き換え、電子情報登録手段 1 4 3 を電子登録手段 1 5 5 に置き換え、電子情報復元手段 1 4 4 を電子情報復元手段 1 5 6 に置き換え、電子財布手段 1 0 1 を電子財布手段 1 5 7 に置き換え、さらに、電子価値情報をバックアップする条件情報を保持するバックアップ条件保管手段 1 5 8 およびバックアップ条件保管手段 1 5 8 から取得したバックアップ条件を解釈して電子財布手段 1 5 7 からバックアップ対象を選択するバックアップ対象抽出手段 1 5 9 とを追加し、端末 1 1 9 を端末 1 5 0 に置き換えたものである。電子情報登録手段 1 4 5 は、バックアップ対象の電子価値情報を自動的に電子金庫手段 1 1 3 に登録して対応する登録証を取得する。これによってバックアップする電子価値情報の選択を、ユーザによる手動選択ではなく事前に設定した条件に基づいて自動的に行なうことができる。

以下、本実施例 1 1 の動作について説明するが、基本的な動作は上記実施例 1 から 6 と同様であるので、以下にはこれらの実施例と異なる部分についてのみ説明する。バックアップ条件保管手段 1 5 8 は、バックアップ条件情報を保持し、その条件情報に基づいて、バックアップする電子価値情報を決定する。本実施例 1 1 では、バックアップ条件情報には初期設定が存在し、また条件情報をユーザが作成・変更できるものとする。バックアップ条件情報としては、電子価値情報の種類や容量、電子財布記憶手段 1 0 2 の空きメモリ容量、電子価値情報の有効期限、電子価値情報の保持開始時間等およびそれらの組み合わせを用いることができる。なお、電子価値情報が持つ情報の項目にあわせて、前記した以外の情報をバックアップ条件に用いても良い。

バックアップ条件情報の例を図 1 9 と図 2 0 で示す。図 1 9 は電子財布記憶手段 1 0 2 上の電子価値情報群の例である。ここでバックアップ条件を映画のチケットとした場合、図 2 0 (a) は上記バックアップ条件に対応する電子価値情報群を示す。本日の日付を 2 0 0 0 年 3 月 1 5 日として、一ヶ月以内に使用可能な日がないことをバックアップ条件とした場合の対応する電子価値情報群は図 2 0 (b) で示される。

次に、このようなバックアップ条件に基づくバックアップ対象抽出手段 1 5 9 による電子価値情報の抽出手順について説明する。

(2-1) バックアップ対象抽出手段 1 5 9 が電子財布手段 1 5 7 に電子価値情報のリストを要求する。

(2-2) 電子財布手段 1 5 7 が電子財布記憶手段 1 0 2 を参照し、電子価値情報のリストを構成する。

(2-3) 電子財布手段 1 5 7 が電子価値情報のリストをバックアップ対象抽出手段 1 5 9 に返す。

(2-4) バックアップ対象抽出手段 1 5 9 は登録されたバックアップ条件とリストを照合し、バックアップ対象電子価値情報リストを生成する。

(2-5) バックアップ対象抽出手段 1 5 9 は電子財布手段 1 5 7 にバックアップ対象電子価値情報リストを渡す。

(2-6) 電子財布手段 1 5 7 は電子財布記憶手段 1 0 2 からバックアップ対象電子価値情報リストで指定された電子価値情報群を取得する。

(2-7) 電子価値情報群に含まれるすべての電子価値情報をそれぞれ暗復号化手段 1 0 5 を用いて暗号化し、暗号化電子価値情報群を生成する。

(2-8) 暗号化電子価値情報群に含まれるすべての暗号化電子価値情報を電子情報登録手段 1 5 5 から端末 1 6 0 を経由して、電子金庫手段 1 1 3 にバックアップする。

(2-9) 電子金庫手段 1 1 3 から暗号化電子価値情報群に対応する登録証群を端末 1 6 0 から電子情報復元手段 1 5 6 を経由して電子財布手段 1 5 7 に渡す。

(2-10) 電子財布手段 1 5 7 は登録証群を電子財布記憶手段 1 0 2 に保管し、電

子財布記憶手段 1 0 2 上から電子価値情報群に含まれる電子価値情報をすべて削除する。

(2-11) 電子財布記憶手段 1 5 7 は端末 1 6 0 に完了を通知する。

バックアップ対象抽出手段 1 5 9 を起動させるタイミングとしては、例えば一定時間ごとにバックアップ対象抽出手段 1 4 9 を起動して、自動的に上記(2-1)から(2-11)で示した手順に従ってバックアップを開始してもよい。または、新規の電子価値情報が電子財布記憶手段に登録される時やバックアップされていた電子価値情報を復元する時に、電子財布記憶手段 1 0 2 の記憶容量が不足する場合にバックアップ対象抽出手段 1 5 9 が自動的に前記手順にしたがってバックアップを開始してもよい。または、ユーザによる起動要求があった場合に、バックアップ対象抽出手段 1 5 9 が自動的に上記手順にしたがってバックアップを開始してもよい。または、上記の条件の組み合わせによって、バックアップ対象抽出手段 1 5 9 が自動的に上記手順にしたがってバックアップを開始してもよい。

また、電子財布記憶手段 1 0 2 の記憶容量不足の場合、現在の電子財布記憶手段 1 0 2 に保持された電子価値情報をバックアップ条件情報に基づいてバックアップする処理を行なった上で、新規の電子価値情報の登録やバックアップ済みの電子価値情報の復元を継続することと、新規の電子価値情報の登録やバックアップ済み電子価値情報の復元を中断することと、手動で現在の電子財布記憶手段 1 0 2 に保持された電子価値情報を選択しバックアップする処理を行なった上で、新規の電子価値情報の登録やバックアップ済みの電子価値情報の復元を継続することを、端末 1 6 0 を操作するユーザに選択させても良い。

実施例 1 2

次に、図 2 1 を用いて、本発明の請求項 2 2、2 3 に係る第 1 2 の実施例について説明する。図 2 1 は本実施例 1 2 における電子情報バックアップシステムの一例を示した構成図であり、本システムは実施例 3 (図 1 0) で示されたシステムの端末 1 1 4 を端末 1 5 3 に置き換え、IC カード 5 0 2 を IC カード 5 0 9 に置き換え、電子情報登録手段 1 2 0 を電子情報登録手段 1 6 1 に置き換え、電子情報復元手段 1 2 1 を電子情報復元手段 1 6 2 に置き換え、さらに、電子金庫

手段 1 1 3 を電子金庫手段 1 6 4 に置き換え、電子金庫手段 1 2 3 を電子金庫手段 1 6 5 に置き換えて、2つの電子金庫手段 1 6 4 と 1 6 5 とを通信回線で接続したものである。さらに、端末 1 6 3 に、実施例 9（図 1 6）に示された所有者情報入力手段 1 4 5、所有者認証情報保管手段 1 4 8、所有者認証手段 1 4 9 を接続したものである。

以下、本実施例 1 2 の動作について説明するが、基本的な動作は上記実施例 3 および 9 と同様であるので、以下にはこれらの実施例と異なる部分についてのみ説明する。所有者情報入力手段 1 4 5、所有者認証情報保管手段 1 4 8、所有者認証手段 1 4 9 を用いて、復号鍵を登録した別の電子金庫手段 1 6 5 に対する所有者認証が成功したとき、この別の電子金庫手段 1 6 5 が電子価値情報を登録した電子金庫手段 1 6 4 と通信を行って暗号化電子情報を取得する。端末 1 6 3 は、別の電子金庫手段 1 6 5 から暗号化電子情報を取得して、電子情報復元手段 1 6 2 に送る。電子情報復元手段 1 6 2 は、暗号化電子価値情報を復号して電子財布手段 1 0 1 上に復元する。一方、暗復号化手段 1 0 5 が、新しい暗号鍵と復号鍵の鍵ペアを生成し、この新しい暗号鍵を用いて電子財布手段 1 0 1 上の電子価値情報を再度暗号化し、電子情報登録手段 1 6 1 が、この新暗号化電子価値情報を電子金庫手段 1 6 4 に端末 1 6 3 を経由して送って登録証を取得するとともに、新しい復号鍵を別の電子金庫手段 1 6 5 に送って同様に登録証を取得する。

このように、本実施例 1 2 では、安全のために電子価値情報と復号鍵を別別の電子金庫手段に預けた場合に、復号鍵を紛失した時や端末が破壊された時には、認証によって正当な情報保持者と認定されることを条件に、電子金庫手段同士が通信を行なって、電子価値情報と復号鍵とを合わせて端末に送り返してくるので、電子価値情報を復元することができる。また、電子価値情報を直ぐに利用しない場合は、新たな暗号鍵を用いて電子価値情報を暗号化し、それを一方の電子金庫手段に送るとともに、復号鍵を他方の電子金庫手段に送ることにより、従前の状態に戻すことができる。

以上説明した各実施例において、電子情報復元手段が登録証を提示して対応する電子価値情報を電子財布手段上に復元する時、または新規の電子価値情報を電

子財布手段上に登録する時に、復元に十分な容量が電子財布記憶手段上に残っていない場合、容量不足をユーザに対して提示して復元作業を中断することができる。

また、上記各実施例において、電子情報登録手段が、電子財布手段から取得した電子価値情報を電子金庫手段に登録して対応する登録証を取得し、登録証が電子財布手段に正常に登録された時は、電子情報登録手段が、電子財布手段から電子価値情報を削除する。また、電子情報復元手段が、電子財布手段から取得した登録証を提示して電子金庫手段から対応する電子価値情報を取得し、電子価値情報を電子財布手段上に正常に復元した時は、電子情報復元手段が、電子財布手段から登録証を削除するとともに、電子金庫手段から電子価値情報を削除する。

また、上記各実施例において、バックアップを行うための起動トリガを、携帯端末を充電台に置いた時、携帯端末が所定時間使用されていない時、携帯端末のバッテリー容量が所定値以下に落ちた時、または所定時間毎、例えば携帯端末を使用していない夜中の23時、またはICカードのメモリー容量が所定値以下に落ちた時、または電子価値情報の利用可能期限、例えば1週間以上先の電子価値情報をバックアップする、等を基準にかけることにより、効率のよいバックアップを行うことができる。

また、バックアップから復元するための起動トリガを、携帯端末の電波受信状態が改善された時、携帯端末のバッテリー容量が所定値以上に回復した時、または所定時間毎、例えば携帯端末を使用可能な毎朝6時、またはICカードのメモリー容量が所定値以上に回復した時、または電子価値情報の利用可能期限、例えば明日から使用可能な電子価値情報を今日復元する、等を基準にかけることにより、効率のよいバックアップ復元を行うことができる。

また、上記各実施例に記載した電子財布手段、電子金庫手段、電子情報登録手段、電子情報復元手段等の制御プログラムをソフトウェアで実現して、磁気ディスク、光磁気ディスク、ROM、DVR OMなどの記録媒体に記録することにより、電子計算機による読み取りが可能になる。

請 求 の 範 囲

1. 電子価値情報を管理する電子財布手段と、
前記電子財布手段固有の記憶領域である電子財布記憶手段と、
電子価値情報の登録を受け付けて登録証を生成して発行し、前記登録証の提示によって対応する前記電子価値情報を取り出すことができる電子金庫手段と、
前記登録証に対応づけて前記電子価値情報を保持する電子金庫手段固有の記憶領域である電子金庫記憶手段と、
前記電子金庫手段に前記電子価値情報を登録して前記登録証を取得する電子情報登録手段と、
前記電子金庫手段に前記登録証を提示して前記電子価値情報を取得する電子情報復元手段とを備え、
前記電子情報登録手段が、前記電子財布手段より取得した電子価値情報を前記電子金庫手段に登録して対応する前記登録証を取得し、前記登録証を前記電子財布手段に登録することと、
前記電子情報復元手段が、前記電子財布手段より取得した前記登録証を前記電子金庫手段に提示して対応する前記電子価値情報を取得し、前記電子財布手段上に復元することを特徴とする電子情報バックアップシステム。
2. 前記電子金庫手段が、登録を要求された電子価値情報の部分情報を含んだ登録証を生成することを特徴とする請求項1に記載の電子情報バックアップシステム。
3. 前記電子金庫手段が、自分自身に対するポイント情報を含んだ登録証を生成することによって、複数の電子金庫手段に対して電子価値情報の登録を可能としたことを特徴とする請求項1に記載の電子情報バックアップシステム。
4. 暗号鍵と復号鍵の組を保持する鍵保管手段と、前記電子価値情報に対し暗号鍵を用いた暗号化と前記復号鍵を用いた復号化を行う暗復号化手段とを備え、前記電子情報登録手段が、前記電子財布手段から取得した電子価値情報を前記暗復号化手段によって暗号化した暗号化電子価値情報を前記電子金庫手段に登録して暗号化電子価値情報登録証を取得することと、前記電子情報復元手段が、前記

暗号化電子価値情報登録証を前記電子金庫手段に提示して対応する前記暗号化電子価値情報を取得し、前記暗復号化手段によって復号化して前記電子価値情報を取得して前記電子金庫手段上に復元することを特徴とする請求項1から3のいずれかに記載の電子情報バックアップシステム。

5. 前記電子情報登録手段が、前記鍵保管手段から鍵情報を取得して前記電子金庫手段に登録して鍵登録証を取得することと、前記電子情報復元手段が、前記鍵登録証を前記電子金庫手段に提示して対応する前記鍵情報を取得し、前記取得した鍵情報を前記鍵保管手段上に復元することを特徴とする請求項4に記載の電子情報バックアップシステム。

6. 前記暗号化した電子価値情報を復号化する復号鍵を、前記電子金庫手段とは別の電子金庫手段に登録して鍵登録証を取得することと、前記電子情報復元手段が、前記鍵登録証を前記別の電子金庫手段に提示して対応する前記鍵情報を取得し、前記取得した鍵情報を前記鍵保管手段上に復元することを特徴とする請求項4に記載の電子情報バックアップシステム。

7. 前記電子価値情報を元の電子価値情報へ復元するための識別子を付加した任意の数の部分電子情報に分割する電子情報分割手段と、前記分割電子情報から元の前記電子価値情報を復元する電子情報合成手段とを備え、前記電子情報登録手段が、前記電子価値情報の分割を前記電子情報分割手段に要求して複数の部分電子情報を取得するとともに、前記部分電子情報の全てまたは一部を電子金庫手段に登録してそれぞれについての部分情報登録証を取得することと、前記電子情報復元手段が、前記部分情報登録証の全てまたは一部をそれぞれの部分情報登録証を発行した電子金庫手段に提示してそれぞれ対応する部分電子情報を取得することと、前記電子情報合成手段が、前記取得した部分電子情報から前記電子価値情報を復元することを特徴とする請求項4に記載の電子情報バックアップシステム。

8. 電子情報登録手段が、電子情報分割手段により分割された複数の分割電子情報をそれぞれ暗復号化手段を用いて暗号化して複数の暗号化分割電子情報を取得し、前記取得した複数の暗号化分割電子情報の全てまたは一部を電子金庫手

段に登録して対応する登録証を取得することを特徴とする請求項7に記載の電子情報バックアップシステム。

9. 電子情報登録手段が、電子価値情報を前記暗復号化手段を用いて暗号化して暗号化電子情報を取得し、前記取得した暗号化電子情報を前記電子情報分割手段を用いて複数の分割暗号化電子情報を取得するとともに、前記複数の分割暗号化電子情報の全てまたは一部を電子金庫手段に登録して対応する登録証を取得することを特徴とする請求項7に記載の電子情報バックアップシステム。

10. 複数の電子価値情報を結合して一つの結合電子情報として出力する電子情報結合手段と、前記結合電子情報を元の複数の電子情報に分割する電子情報結合解除手段とを備え、前記電子情報結合手段が、複数の電子価値情報の組から結合電子情報を生成することと、前記電子情報登録手段が、前記結合電子情報を前記電子金庫手段に登録して対応する結合電子情報登録証を取得することと、前記電子情報復元手段が、前記結合電子情報登録証を提示して電子金庫手段から対応する結合電子情報を取得することと、前記電子情報結合解除手段が、前記結合電子情報から前記電子価値情報の組を取得することを特徴とする請求項7に記載の電子情報バックアップシステム。

11. 前記電子情報分割手段が、前記電子情報登録手段が前記鍵保管手段から取得した鍵情報を複数の部分鍵に分割することと、前記暗復号化手段が、前記電子情報登録手段が前記電子財布手段から取得した電子価値情報を暗号化して暗号化電子情報を取得することと、前記電子情報結合手段が、前記暗号化電子情報と前記部分鍵の一部である部分鍵群Aとから結合電子情報を取得することと、前記電子情報登録手段が、前記結合電子情報と残りの部分鍵である部分鍵群Bとをそれぞれ異なる電子金庫手段に登録して対応する登録証を取得することと、前記電子情報復元手段が、前記登録証を対応する前記電子金庫手段に提示して前記結合電子情報と前記部分鍵群Bとを取得することと、前記電子情報結合解除手段が、前記結合電子情報を前記暗号化電子情報と前記部分鍵群Aとに分離することと、前記電子情報合成手段が、前記部分鍵群Aと前記部分鍵群Bとを合成して鍵情報を生成することと、前記暗復号化手段が、前記暗号化電子情報を復号して前記電

子価値情報を取得することと、前記電子情報復元手段が、前記鍵情報を取得して前記鍵保管手段上に復元するとともに、前記電子価値情報を電子財布手段上に復元することを特徴とする請求項10に記載の電子情報バックアップシステム。

12. 前記電子情報分割手段が、鍵情報を分割して得る部分鍵を暗号鍵と復号鍵の鍵ペアを生成する元となる情報とすることを特徴とする請求項11に記載の電子情報バックアップシステム。

13. 復号鍵を生成するために用いる元の暗号種（たね）情報と、前記暗号種情報から復号鍵を生成する復号鍵生成アルゴリズムとを備え、前記電子情報登録手段が、前記暗号種情報を前記電子金庫手段に登録して対応する暗号種情報登録証を取得することと、前記電子情報復元手段が、前記暗号種情報登録証を提示して前記電子金庫手段から対応する暗号種情報を取得することと、前記暗号復号化手段が、前記暗号種情報に前記復号鍵生成アルゴリズムをかけて復号鍵を生成するとともに、前記電子情報復元手段が取得した前記電子価値情報を前記復号鍵を用いて復号化することを特徴とする請求項4、6、7、10、11のいずれかに記載の電子情報バックアップシステム。

14. 所有者固有の所有者情報を入力する所有者情報入力手段と、前記所有者情報に対応する所有者認証情報を入力する所有者認証情報入力手段とを備え、前記電子情報登録手段が、前記電子価値情報と前記所有者認証情報入力手段より取得した所有者認証情報とを組として前記電子金庫手段に登録することと、前記電子情報復元手段が、前記所有者情報入力手段より取得した所有者情報を前記電子金庫手段に提示して前記所有者認証情報と照合が成功した時に、前記電子価値情報を取得できることを特徴とする請求項1、4、6、7、10、11のいずれかに記載の電子情報バックアップシステム。

15. 所有者固有の所有者情報を入力する所有者情報入力手段と、前記所有者情報に対応する所有者認証情報を保持する所有者認証情報保管手段と、前記所有者情報と前記所有者認証情報とを対照して正当性を検証する所有者認証手段とを備え、前記所有者情報入力手段から入力された所有者情報を前記所有者認証手段に提示して認証を行うことと、その認証結果を用いて前記電子情報登録

手段と電子金庫手段との間の暗号化通信路を構築することと、前記暗号化通信路を通して前記電子情報登録手段が前記電子価値情報を電子金庫手段に登録することと、前記電子金庫手段が前記認証結果に対応する所有者認証情報と前記電子価値情報とを組として電子金庫記憶手段に保持することと、前記電子情報復元手段が前記暗号化通信路を通して前記認証結果に対応する前記所有者認証情報に対応する前記電子価値情報を取得することを特徴とする請求項 1、4、6、7、10、11 のいずれかに記載の電子情報バックアップシステム。

16. 前記所有者情報入力手段と所有者認証手段が一時的に利用する共通鍵を生成し共有することと、前記共通鍵によって所有者情報を暗号化して所有者認証手段に送信することを特徴とする請求項 15 に記載の電子情報バックアップシステム。

17. 前記所有者情報入力手段が所有者認証手段固有の秘密鍵に対応した公開鍵で所有者情報を暗号化することと、前記所有者情報入力手段が前記の暗号化した所有者情報を所有者認証手段に送信することを特徴とする請求項 16 に記載の電子情報バックアップシステム。

18. 所有者認証に用いる認証機器を読み取る認証機器読み取り手段と、前記認証機器の正当性を検証する認証確認手段と、前記認証確認手段が前記認証機器の正当性確認で対照する情報を保持する認証確認情報保管手段とを備え、前記認証機器読み取り手段に接続された認証機器と認証確認手段が相互に正当性を確認することを特徴とする請求項 1、4、6、7、10、11 のいずれかに記載の電子情報バックアップシステム。

19. 所有者認証に用いる認証機器を読み取る認証機器読み取り手段と、前記認証機器の正当性を検証する認証確認手段と、前記認証確認手段が前記認証機器の正当性確認で対照する情報を保持する認証確認情報保管手段とを備え、前記認証機器読み取り手段に接続された認証機器と認証確認手段が相互に正当性を確認することと、その認証結果を用いて電子情報登録手段と電子金庫手段の間の暗号化通信路を構築することと、前記暗号化通信路を通して電子情報登録手段が電子価値情報を電子金庫手段に登録することと、前記電子金庫手段が前記認証結果

に対応する所有者認証情報と前記電子価値情報とを組として電子金庫記憶手段に保持することと、前記電子情報復元手段が前記暗号化通信路を通して前記認証結果に対応する前記所有者認証情報に対応する前記電子価値情報を取得することを特徴とする請求項 1、4、6、7、10、11 のいずれかに記載の電子情報バックアップシステム。

20. 電子価値情報をバックアップする条件情報を保持するバックアップ条件保管手段と、前記バックアップ条件保管手段から取得したバックアップ条件を解釈して前記電子財布手段からバックアップ対象を選択するバックアップ対象抽出手段とを備え、前記電子情報登録手段が前記バックアップ対象の電子価値情報を自動的に前記電子金庫手段に登録して対応する登録証を取得することを特徴とする請求項 1、4、6、7、10、11、14、15、18、19 のいずれかに記載の電子情報バックアップシステム。

21. 電子情報復元手段が登録証を提示して対応する電子価値情報を電子財布手段上に復元する時または新規の電子価値情報を電子財布手段上に登録する時に復元に十分な容量が電子財布記憶手段上に残っていない場合、電子情報登録手段が前記バックアップ対象抽出手段を用いて前記電子財布手段上からバックアップ対象の電子価値情報を選択して前記電子財布金庫手段に登録して対応する登録証を取得することと、前記バックアップ対象の電子価値情報を前記電子財布記憶手段上から削除して空き容量を拡大することと、空き容量を確保が完了した時に前記の電子財布手段上への電子情報の復元または新規登録を継続することを特徴とした請求項 20 に記載の電子情報バックアップシステム。

22. 前記復号鍵を登録した別の電子金庫手段への所有者認証が成功したとき、前記別の電子金庫手段が前記復号鍵以外の電子価値情報を登録した電子金庫手段と通信を行って暗号化電子情報を取得することと、前記電子情報復元手段が前記別の電子金庫手段から前記暗号化された電子価値情報を取得して前記電子財布手段上に復元することを特徴とする請求項 6 に記載の電子情報バックアップシステム。

23. 前記復号鍵を登録した別の電子金庫手段への所有者認証が成功したと

き、前記別の電子金庫手段が前記復号鍵以外の電子価値情報を登録した電子金庫手段と通信を行って暗号化電子情報を取得することと、前記電子情報復元手段が前記別の電子金庫手段から前記暗号化された電子価値情報を取得して前記電子財布手段上に復元することと、前記暗復号化手段が新しい暗号鍵と復号鍵の鍵ペアを生成することと、前記新しい暗号鍵を用いて前記電子価値情報を暗号化して、前記新暗号化電子価値情報を前記電子金庫手段に送るとともに、前記新しい復号鍵を前記別の電子金庫手段に送ることを特徴とする請求項 6 に記載の電子情報バックアップシステム。

24. 前記電子情報復元手段が登録証を提示して対応する電子価値情報を電子財布手段上に復元する時、または新規の電子価値情報を電子財布手段上に登録する時に、復元に十分な容量が電子財布記憶手段上に残っていない場合、容量不足をユーザに対して提示して復元作業を中断することを特徴とした請求項 1 から 23 のいずれかに記載の電子情報バックアップシステム。

25. 前記電子情報登録手段が、前記電子財布手段から取得した電子価値情報を前記電子金庫手段に登録して対応する登録証を取得し、前記登録証が前記電子財布手段に正常に登録された時は、前記電子情報登録手段が、前記電子財布手段から前記電子価値情報を削除することを特徴とする請求項 1 から 24 のいずれかに記載の電子情報バックアップシステム。

26. 前記電子情報復元手段が、前記電子財布手段から取得した登録証を提示して前記電子金庫手段から対応する電子価値情報を取得し、前記電子価値情報を電子財布手段上に正常に復元した時は、前記電子情報復元手段が、前記電子財布手段から前記登録証を削除するとともに、前記電子金庫手段から前記電子価値情報を削除することを特徴とする請求項 1 から 25 のいずれかに記載の電子情報バックアップシステム。

27. 電子価値情報を外部サーバに登録してその登録証を取得するとともに、前記電子価値情報および登録証を記憶媒体に記憶し、前記外部サーバに対して登録証を提示して電子価値情報を復元するバックアップ手段を備えたことを特徴とする電子情報バックアップシステム。

28. 前記登録証に電子価値情報の部分情報を含むことを特徴とする請求項27に記載の電子情報バックアップシステム。

29. 登録要求された電子価値情報を暗号鍵を用いて暗号化して暗号化電子価値情報を取得するとともに、前記暗号化電子価値情報を外部サーバに登録するバックアップ手段を備えたことを特徴とする電子情報バックアップシステム。

30. 復元要求された登録証を外部サーバに提示して対応する暗号化電子価値情報を取得し、前記暗号化電子価値情報を復号鍵を用いて電子価値情報に復元するバックアップ手段を備えたことを特徴とする電子情報バックアップシステム。

31. 登録要求された電子価値情報を分割して複数の部分電子情報を取得し、前記部分電子情報のすべてを任意の数の外部サーバに登録して前記部分電子情報と同数の部分情報登録証を取得するとともに、前記部分情報登録証のすべてを記憶媒体に記憶するバックアップ手段を備えたことを特徴とする電子情報バックアップシステム。

32. 前記すべての部分情報登録証を外部サーバに提示して同数の部分電子情報を取得し、前記部分電子情報のすべてを合成して元の電子価値情報を復元して前記記憶媒体に記憶することを特徴とする請求項31に記載の電子情報バックアップシステム。

33. 電子価値情報を復号鍵に対応した暗号鍵で暗号化して暗号化電子価値情報を取得し、前記復号鍵を分割して複数の部分復号鍵とし、前記部分復号鍵の一以上と前記暗号化電子価値情報とを結合して結合電子情報を取得し、前記結合電子情報を外部サーバに登録して結合登録証を取得し、残りの部分復号鍵を別の外部サーバに登録し、前記結合登録証を記憶媒体に記憶するバックアップ手段を備えたことを特徴とする電子情報バックアップシステム。

34. 前記結合登録証を前記外部サーバに提示して前記結合電子情報を取得し、前記結合電子情報を結合解除して前記暗号化電子価値情報と一以上の部分復号鍵に分解し、前記残りの部分復号鍵を前記別の外部サーバから取得し、前記分解した部分復号鍵と前記取得した部分復号鍵とを合成して元の復号鍵に復元し、前記復元した復号鍵を用いて前記暗号化電子価値情報を元の電子価値情報に復元

して前記記憶媒体に記憶することを特徴とする請求項 3 3 に記載の電子情報バックアップシステム。

3 5. 電子価値情報に対応する登録証を外部サーバから取得した時に、前記登録証に対応する前記電子価値情報を前記記憶媒体から削除することを特徴とする請求項 2 7 から 3 4 のいずれかに記載の電子情報バックアップシステム。

3 6. 予め設定されたバックアップ条件を解釈して前記記憶媒体からバックアップ対象の電子価値情報を選択し、前記選択された電子価値情報を自動的に前記外部サーバに登録して対応する登録証を取得することを特徴とする請求項 2 7 から 3 5 のいずれかに記載の電子情報バックアップシステム。

3 7. 認証用情報と電子価値情報とを組として前記外部サーバに登録することを特徴とする請求項 2 7 から 3 6 のいずれかに記載の電子情報バックアップシステム。

3 8. 入力された所有者情報を前記外部サーバに提示して前記外部サーバに登録された認証用情報と一致した時に、前記電子価値情報を取得可能とすることを特徴とする請求項 3 7 に記載の電子情報バックアップシステム。

3 9. 入力された所有者情報に対応する所有者認証情報を記憶媒体に保持し、前記所有者情報と前記所有者認証情報とを照合して一致した時に、前記電子価値情報を取得可能とすることを特徴とする請求項 2 7 から 3 6 のいずれかに記載の電子情報バックアップシステム。

4 0. 前記所有者情報と前記所有者認証情報とが一致した時に、前記外部サーバとの間に暗号化通信路を構築し、前記所有者情報に対応する電子価値情報を取得可能とすることを特徴とする請求項 3 9 に記載の電子情報バックアップシステム。

4 1. 所有者認証情報を記録した IC カードを読み取ってその認証情報を外部サーバに送り、前記外部サーバが前記認証情報の正当性を確認した時に、前記電子価値情報を取得可能とすることを特徴とする請求項 2 7 から 3 6 のいずれかに記載の電子情報バックアップシステム。

4 2. 前記認証情報の正当性を確認した時に、前記外部サーバとの間に暗号

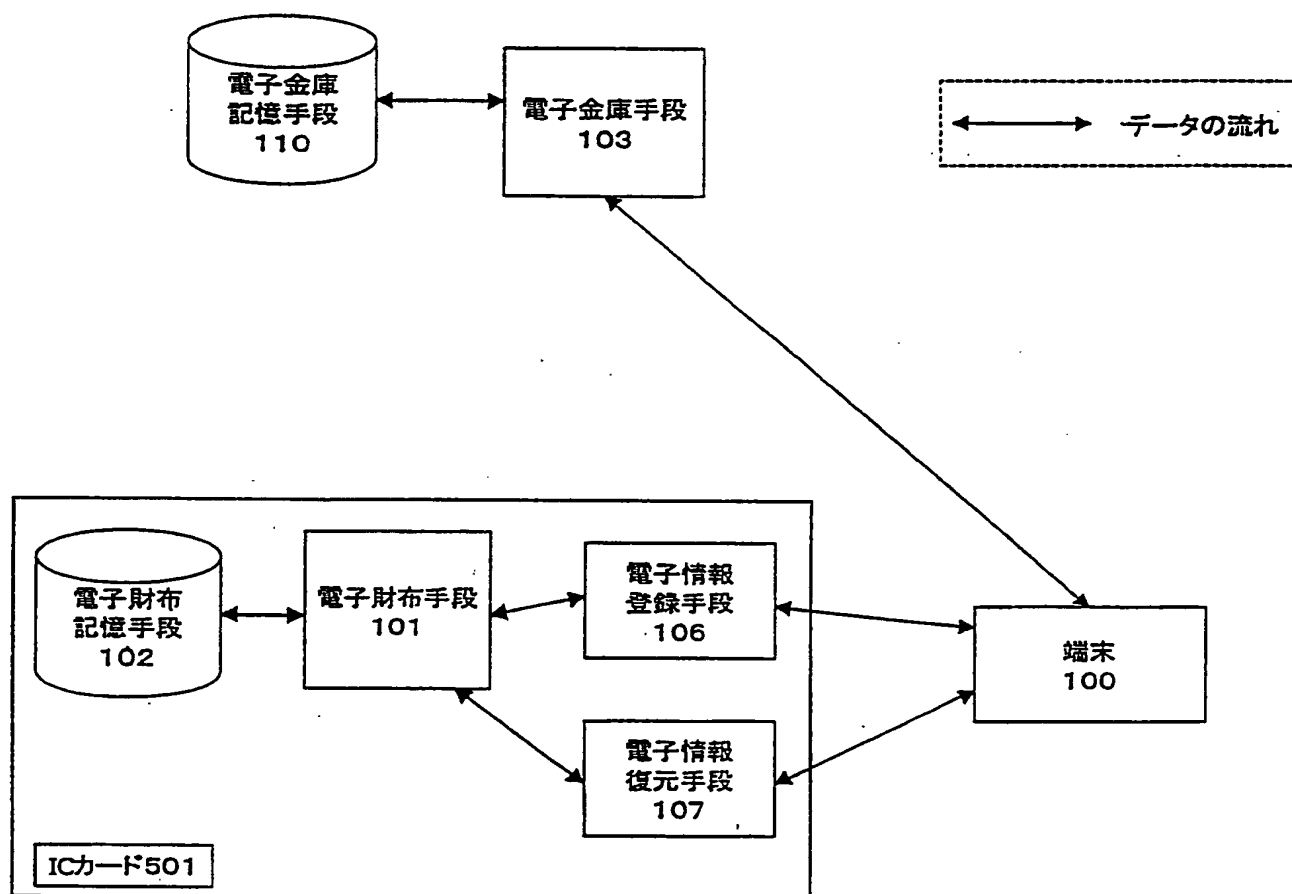
化通信路を構築し、前記認証情報に対応する電子価値情報を取得可能とすることを特徴とする請求項 4 1 に記載の電子情報バックアップシステム。

4 3. 復号鍵を登録した別の外部サーバへの所有者認証が成功した時に、前記別の外部サーバが前記復号鍵以外の電子価値情報を登録した外部サーバと通信を行って暗号化電子情報を取得して前記復号鍵と結合することを特徴とする請求項 2 7 または 3 6 のいずれかに記載の電子情報バックアップシステム。

4 4. 前記暗号化電子情報を取得して復号した後、新たな暗号鍵を用いて前記電子価値情報を暗号化し、それを前記外部サーバに登録とともに、復号鍵を別の外部サーバに登録することを特徴とする請求項 4 3 に記載の電子情報バックアップシステム。

THIS PAGE BLANK (USPTO)

図 1



THIS PAGE BLANK (USPTO)

図 2

電子価値情報201

情報種別	映画チケット
名前	映画タイトル
単価	A円
数	B
合計金額	A×B円
場所	劇場名
有効期限	C～D
備考

(a)

ダイジェスト302

情報種別	映画チケット
名前	映画タイトル
数	B
有効期限	C～D
場所	劇場名

(b)

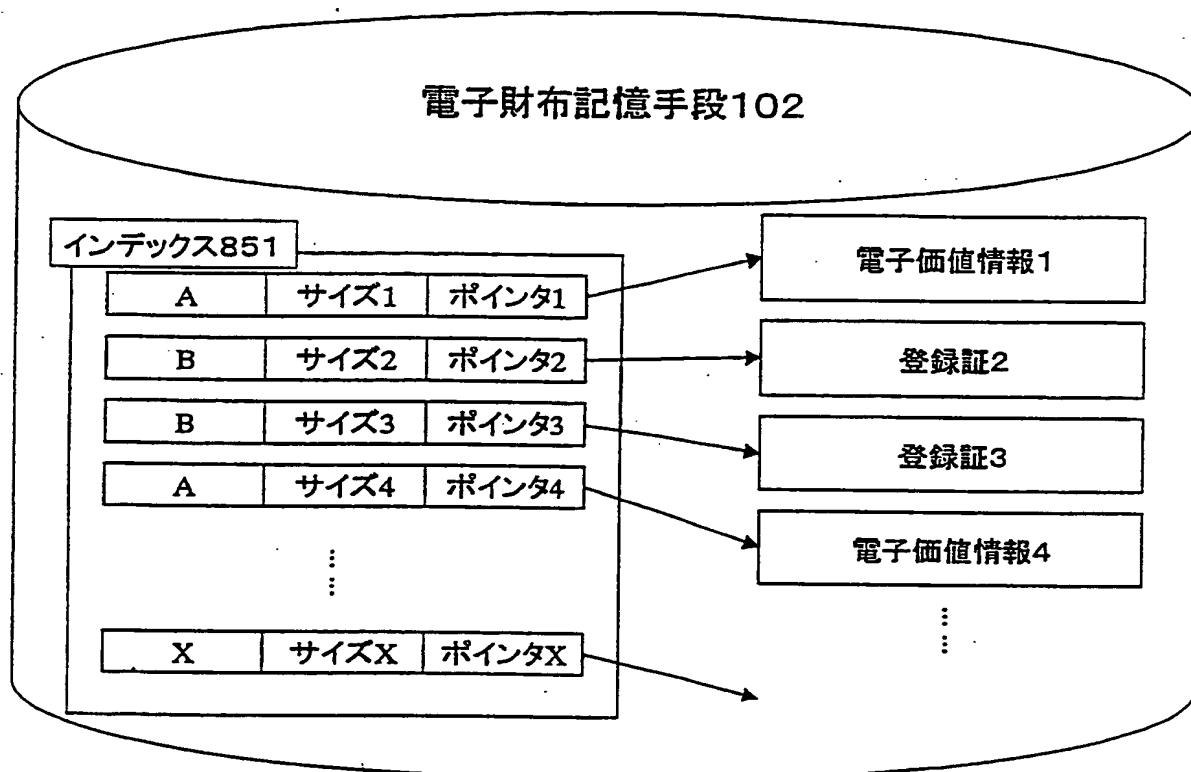
登録証301

ダイジェスト302	ハッシュ値X1	カウンタ値Y1
-----------	---------	---------

(c)

THIS PAGE BLANK (USPTO)

図 3

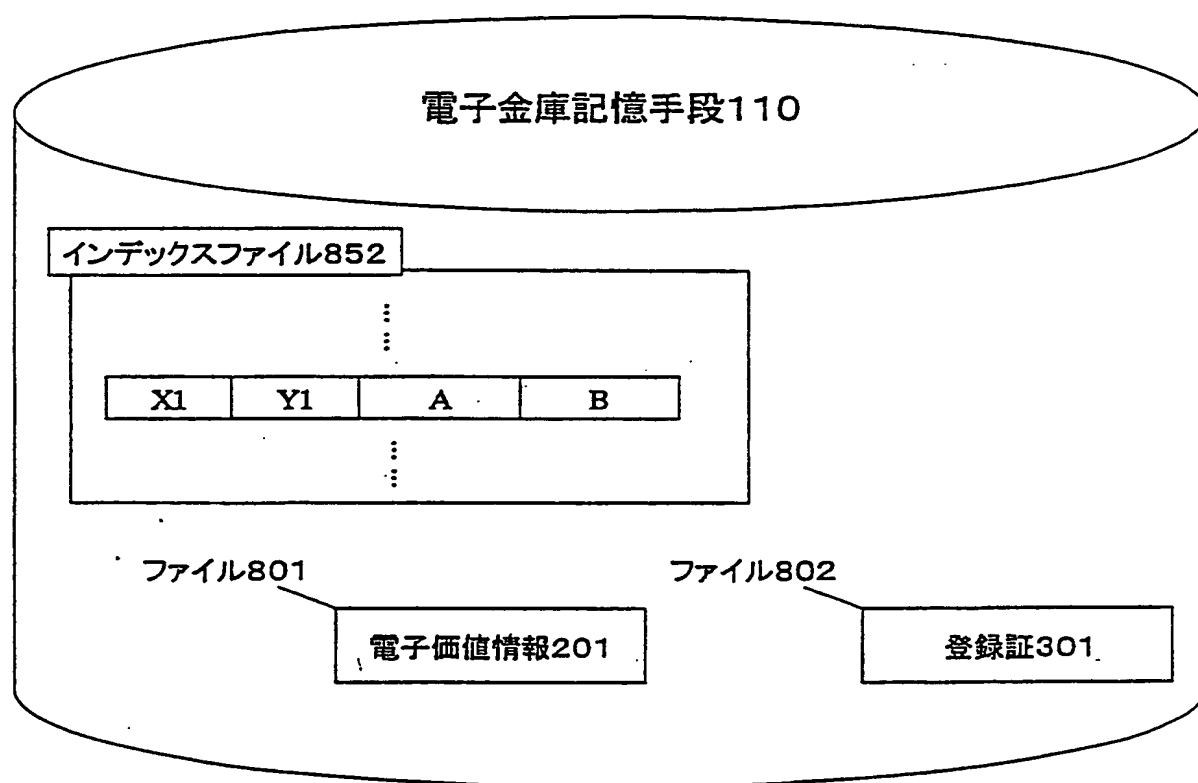


A ... 電子価値情報へのポインタを表す記号
B ... 登録証へのポインタを表す記号

→ ポインタが指すデータの実体

THIS PAGE BLANK (USPTO)

図 4

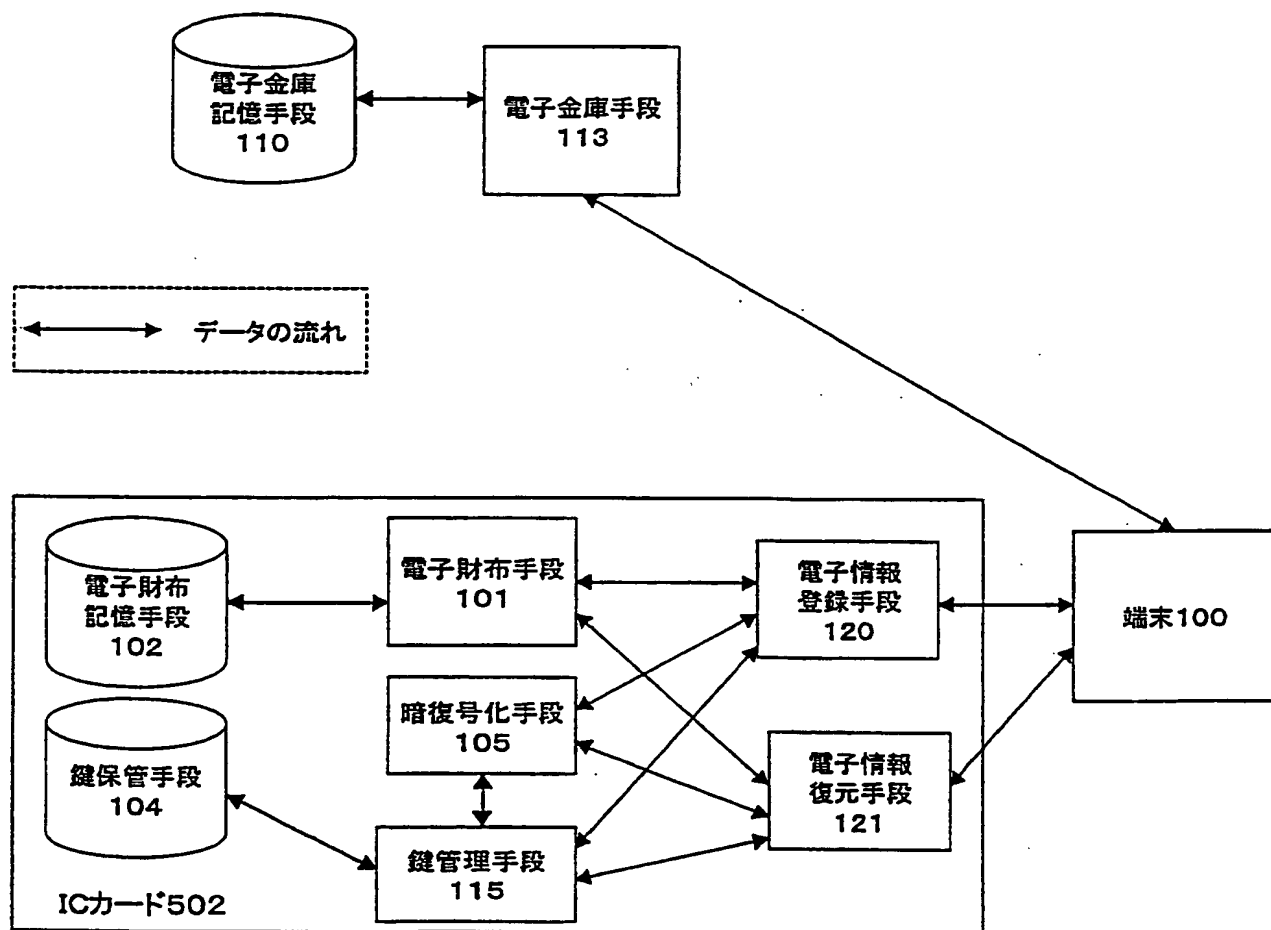


A ... ファイル801のパス情報
B ... ファイル802のパス情報

X1 ... 登録証301の構成要素のハッシュ値
Y1 ... 登録証301の構成要素のカウント値

THIS PAGE BLANK (USPTO)

図 5



THIS PAGE BLANK (USPTO)

図 6

登録電子価値情報203

情報種別	映画チケット
名前	映画タイトル
数	B
場所	劇場名
有効期限	C~D
ダイジェスト302	
暗号化電子価値情報202	
署名303	

(a)

登録証304

ダイジェスト302	ハッシュ値X2	カウンタ値Y2
-----------	---------	---------

(b)

THIS PAGE BLANK (USPTO)

図 7

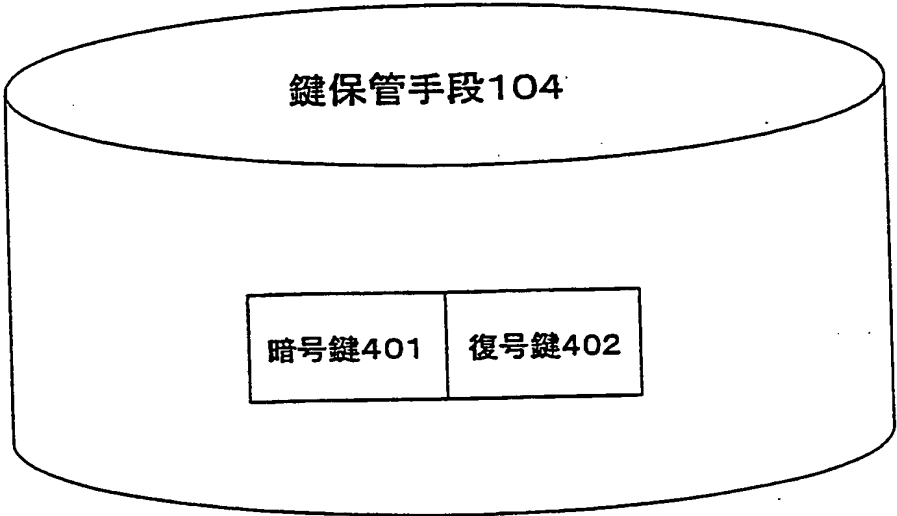
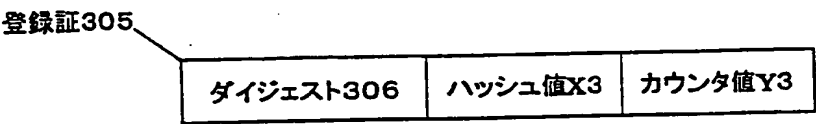
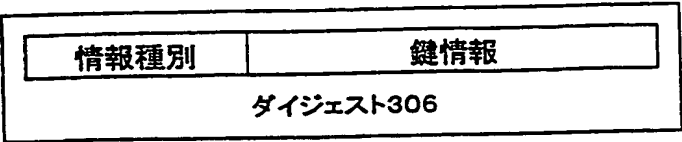


図 8



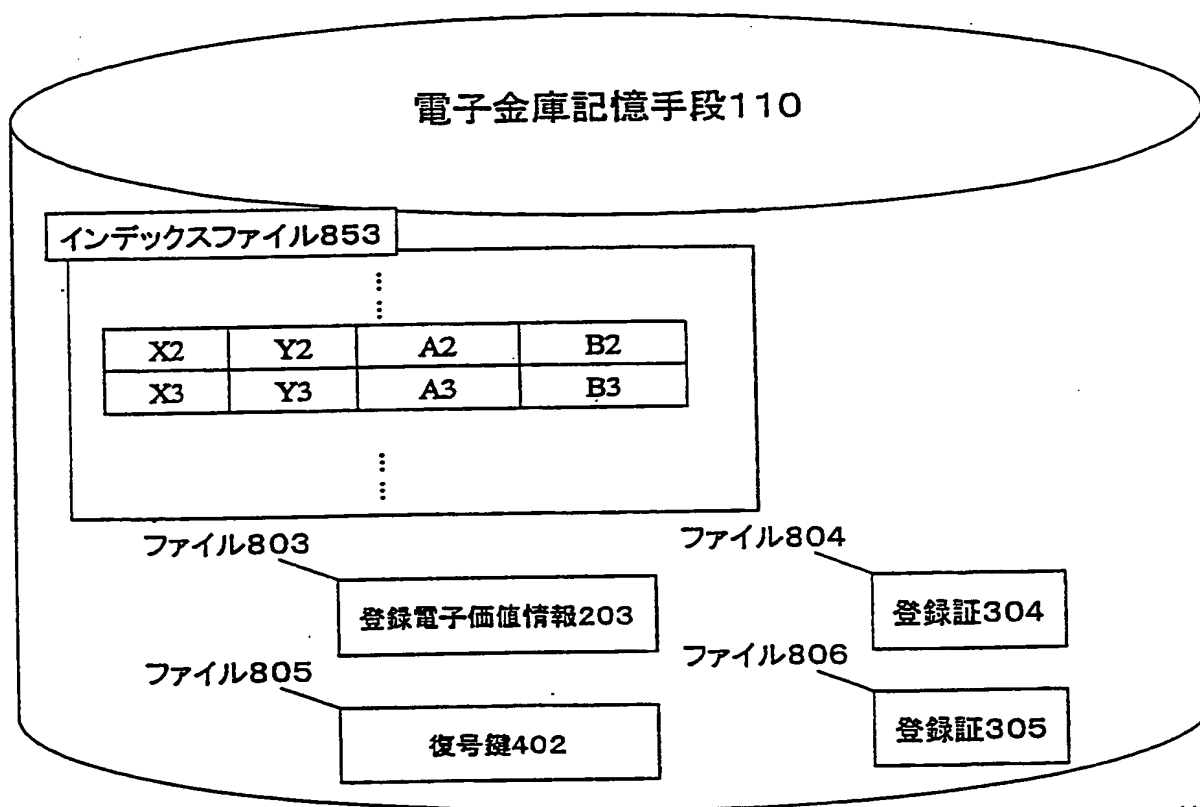
(a)



(b)

THIS PAGE BLANK (USPTO)

図 9

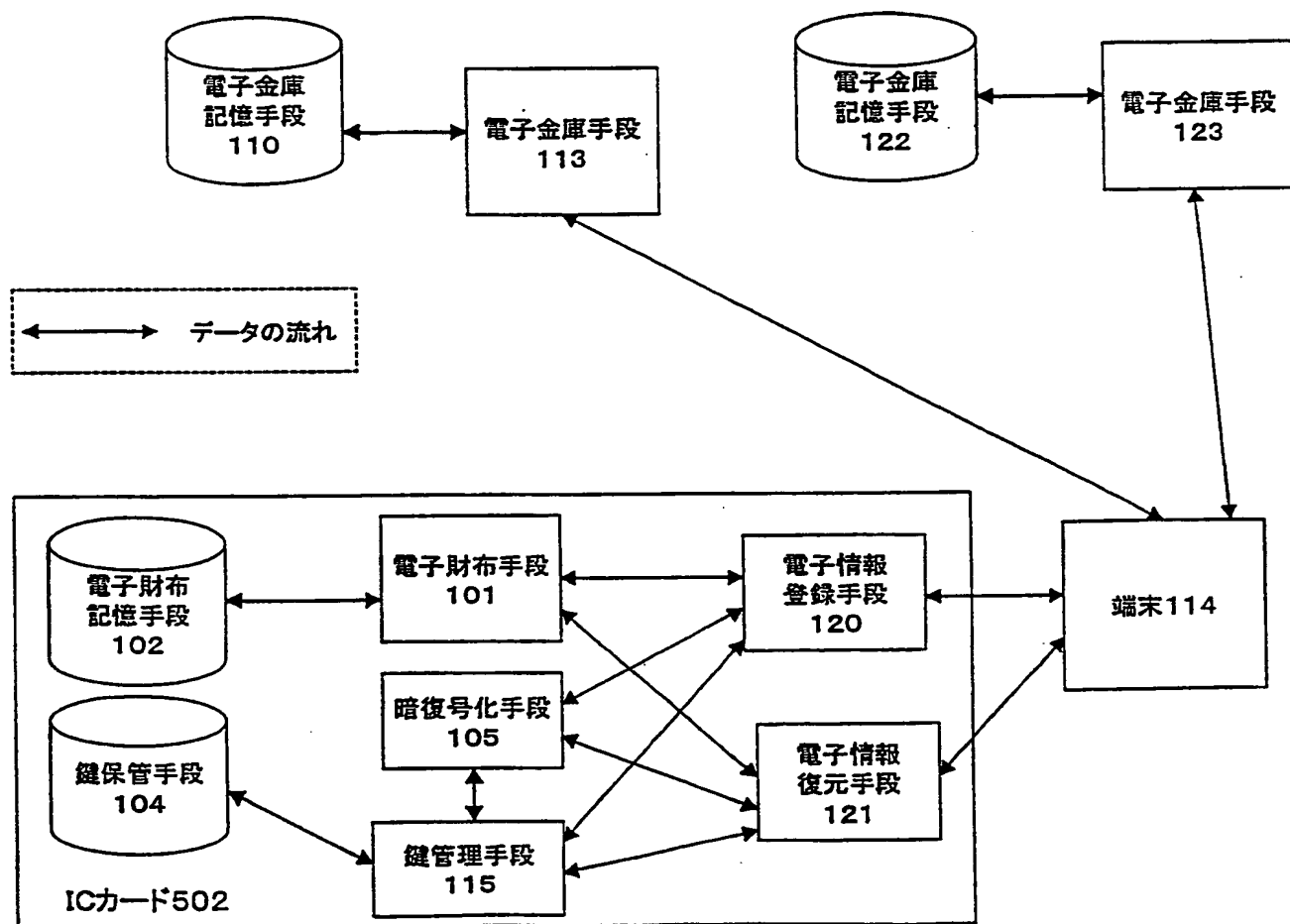


A2 ... ファイル803のパス情報
B2 ... ファイル804のパス情報
A3 ... ファイル805のパス情報
B3 ... ファイル806のパス情報

X2 ... 登録証304の構成要素のハッシュ値
Y2 ... 登録証304の構成要素のカウント値
X3 ... 登録証305の構成要素のハッシュ値
Y3 ... 登録証305の構成要素のカウント値

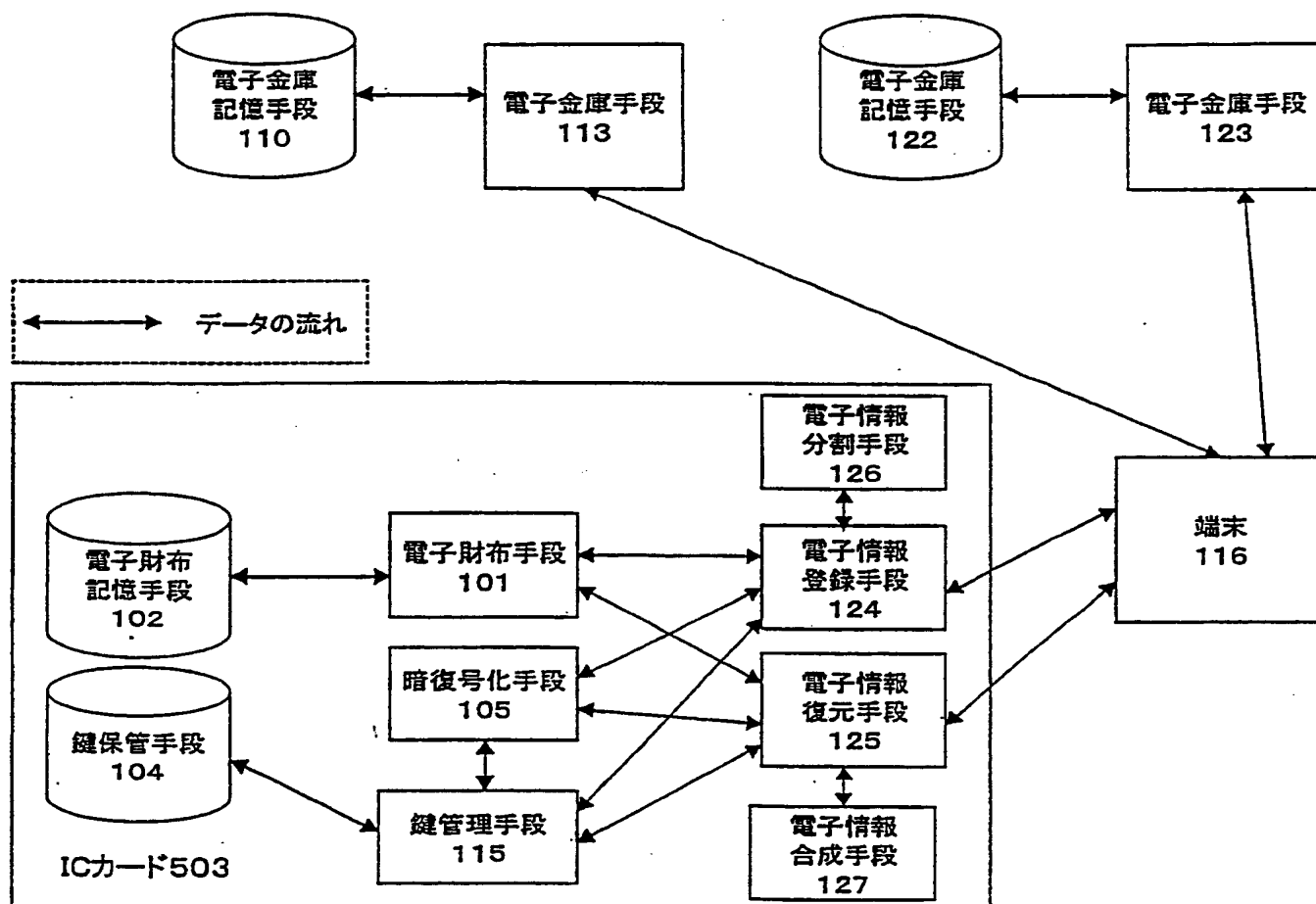
THIS PAGE BLANK (USPTO)

図 10



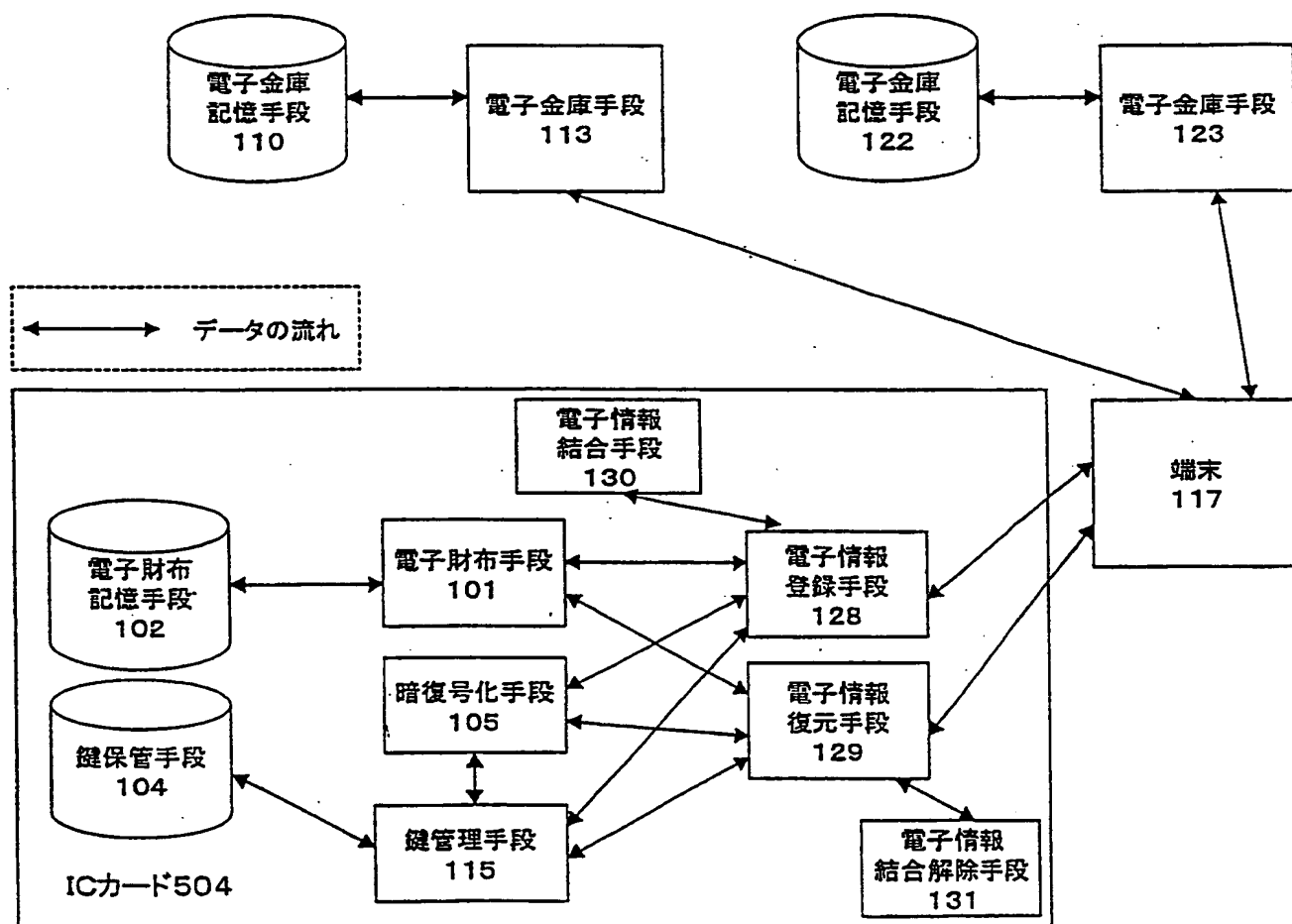
THIS PAGE BLANK (USPTO)

図 11



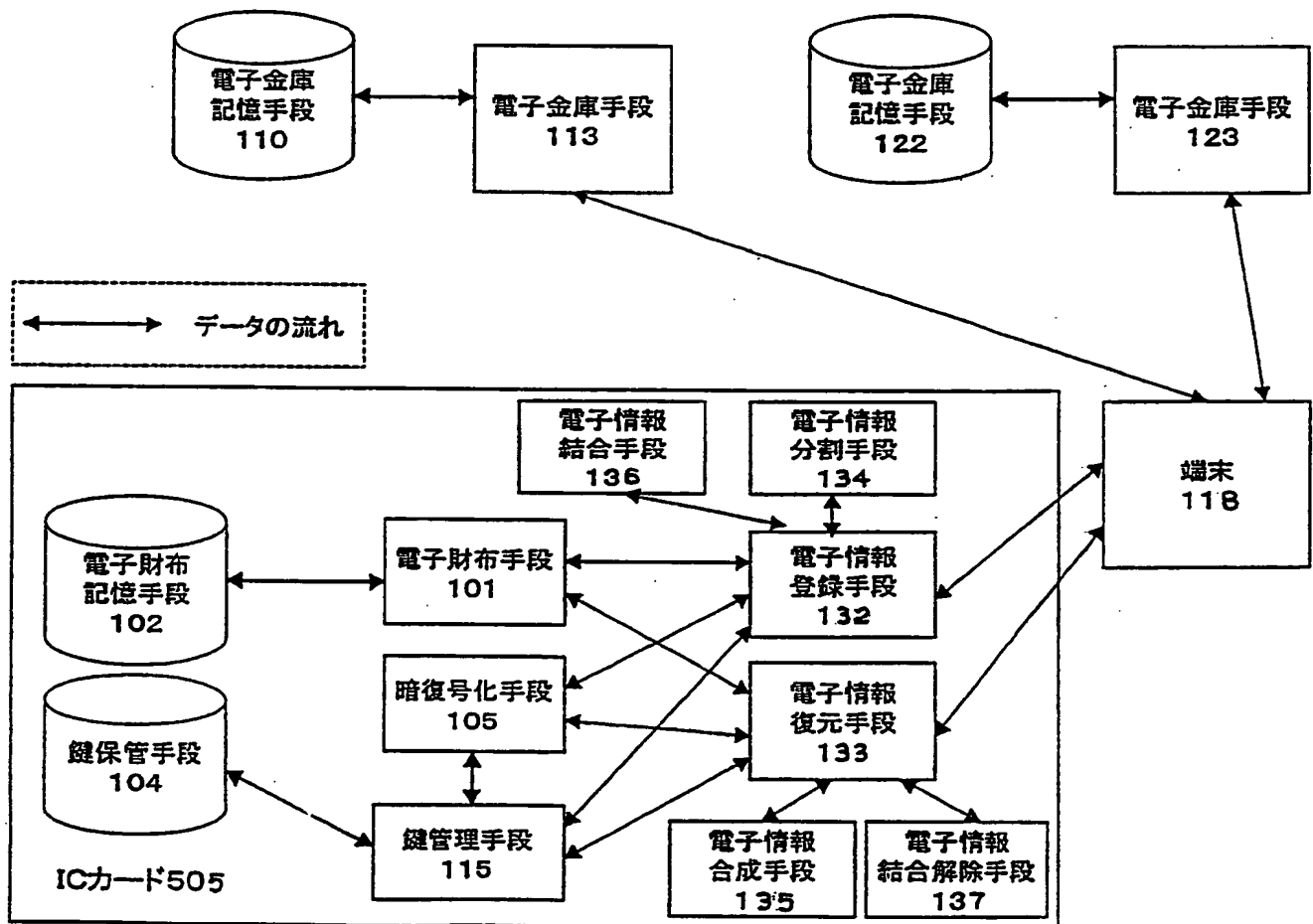
THIS PAGE BLANK (USPTO)

図 12



THIS PAGE BLANK (USPTO)

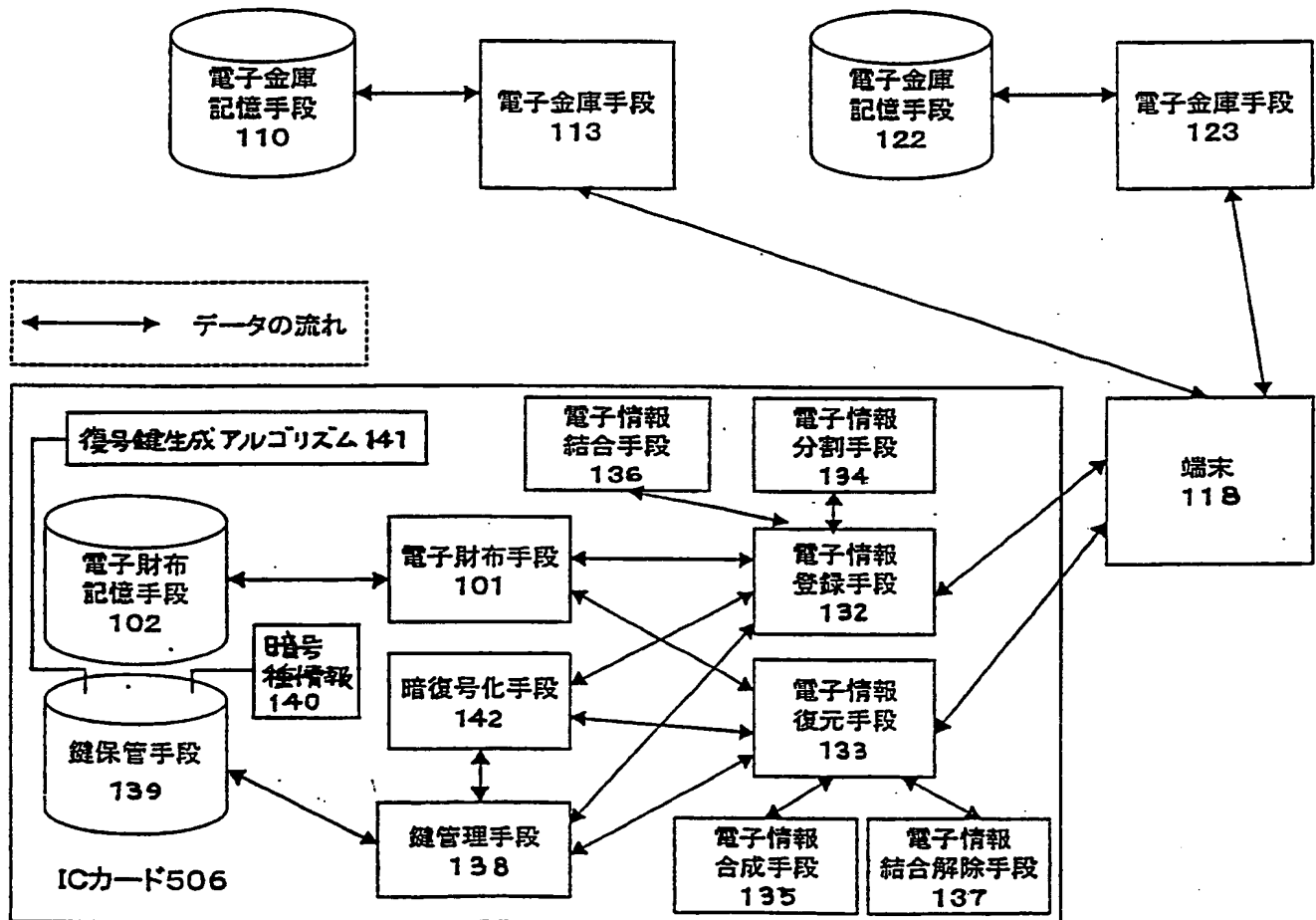
図 13



THIS PAGE BLANK (USPTO)

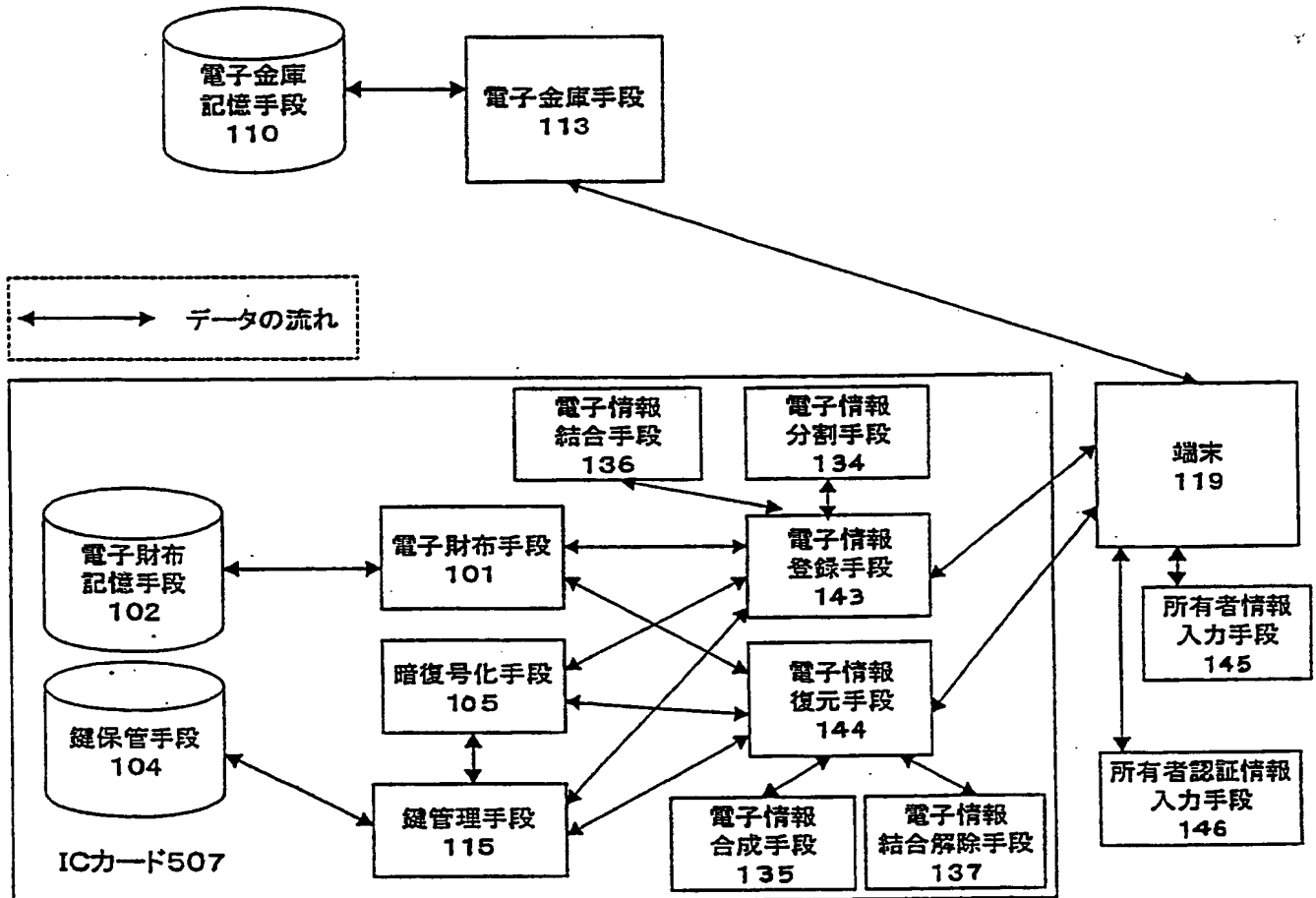
13 / 19

図 14



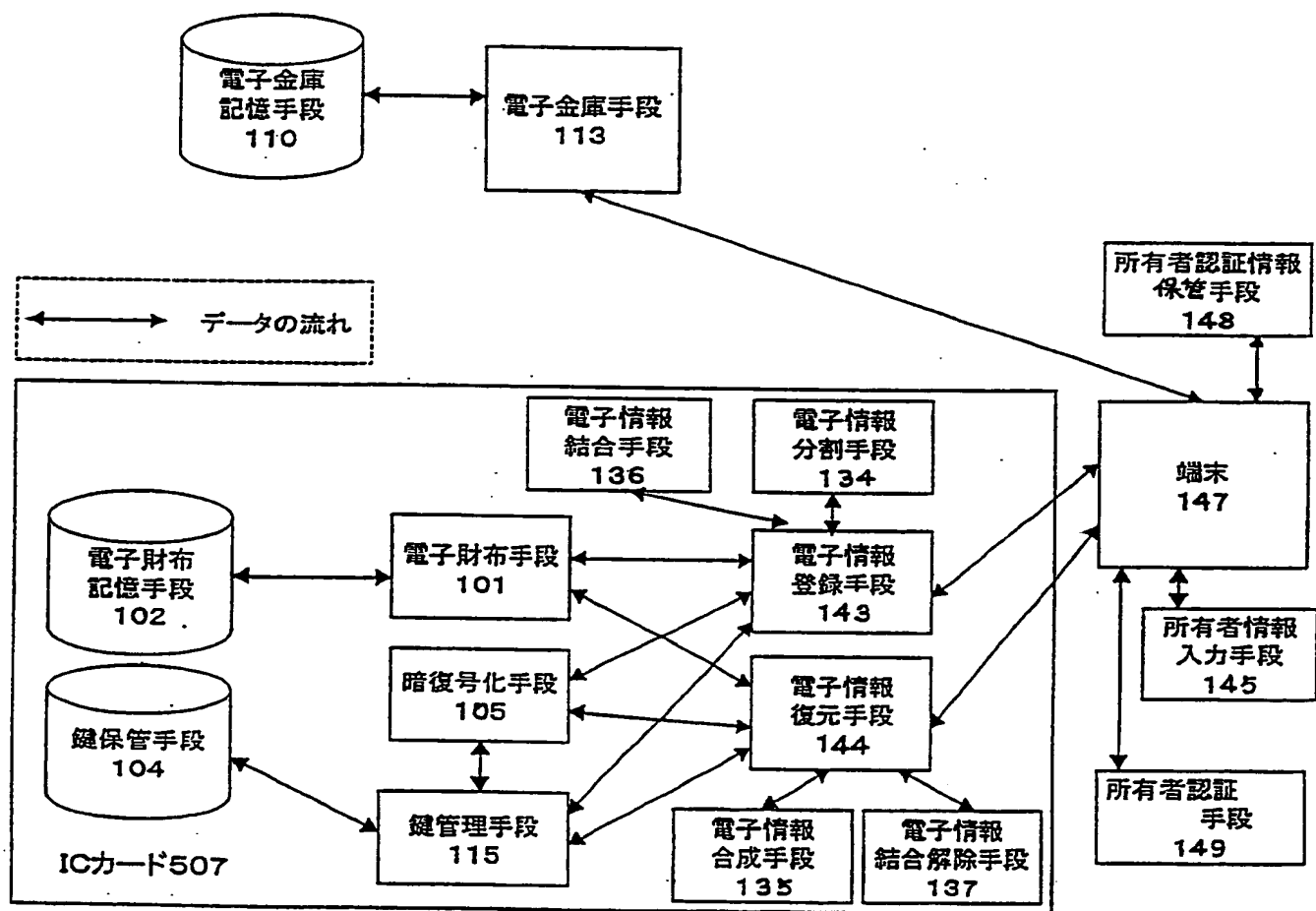
THIS PAGE BLANK (USPTO)

図 15



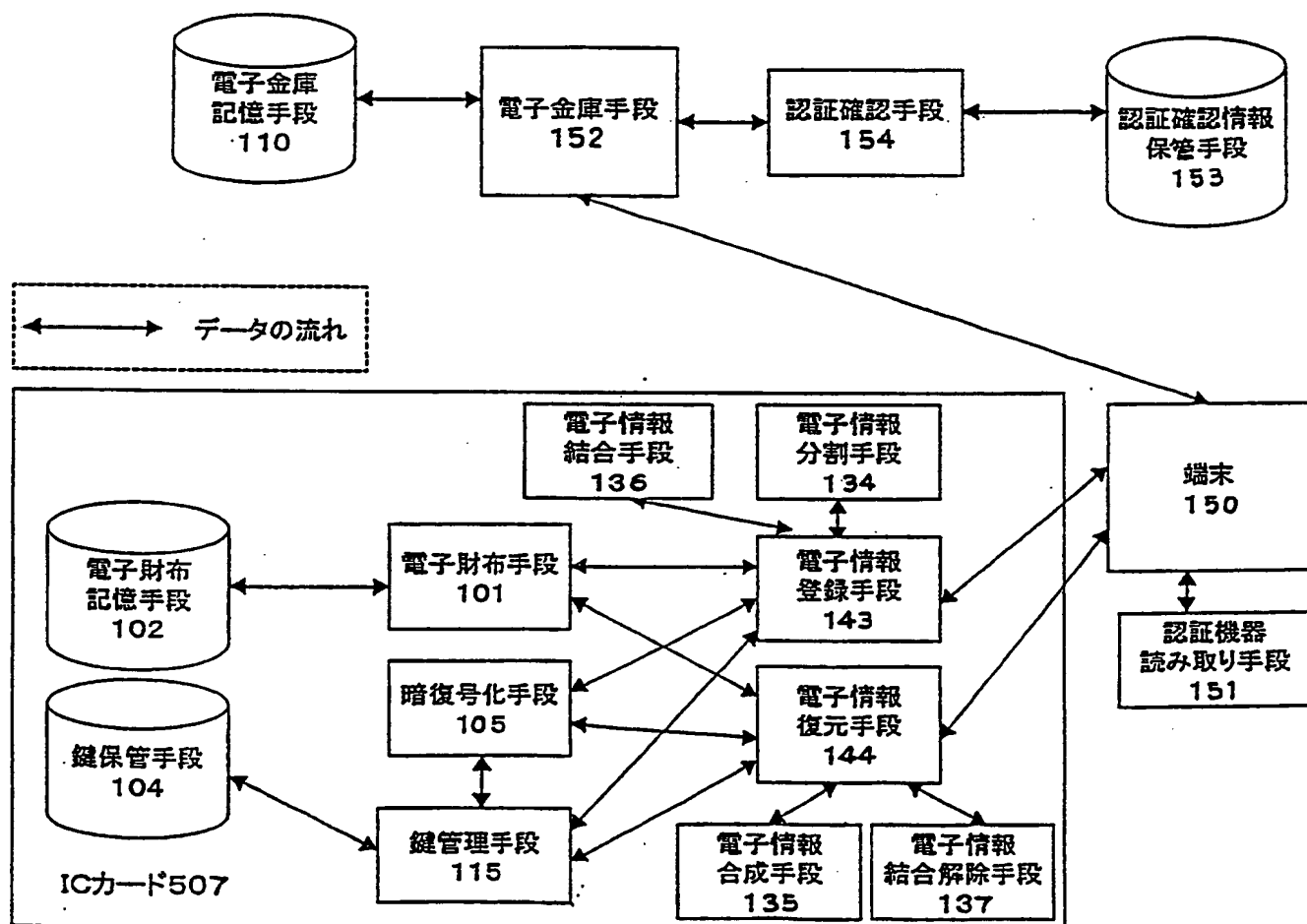
THIS PAGE BLANK (USPTO)

図 16



THIS PAGE BLANK (USPTO)

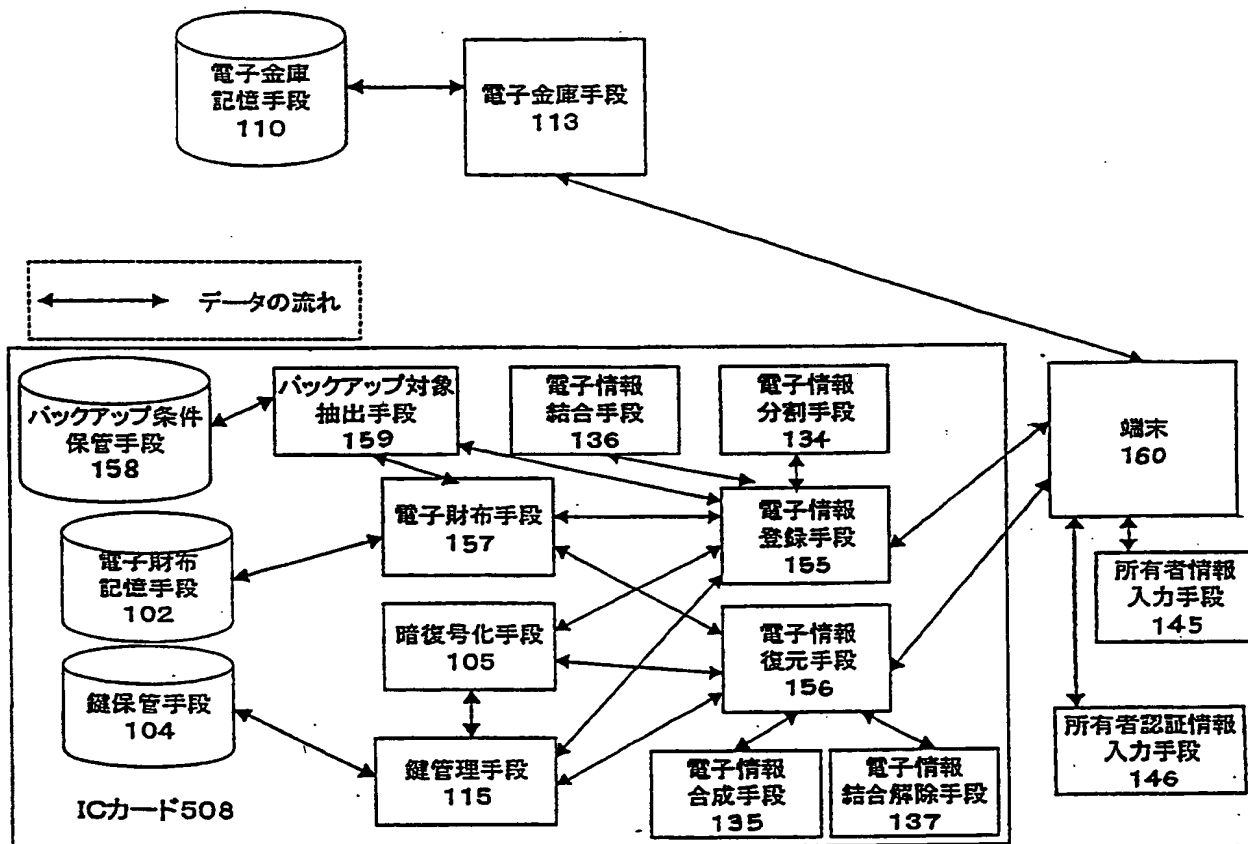
図 17



THIS PAGE BLANK (USPTO)

17/19

図18



THIS PAGE BLANK (USPTO)

18 / 19

図 19

情報種別	映画チケット	コンサートチケット
名前	A	C
単価	1600円	4500円
数	1	2
合計金額	1600円	9000円
場所	B	D
有効期間	2000年4月1日～2000年5月31日	2000年4月29日～2000年4月29日
残金	0円	0円

プリペイドカード	映画チケット
E	G
1000円	1600円
1	2
1000円	3200円
F	H
無期限	2000年5月1日～2000年6月30日
800円	0円

図 20

映画チケット	映画チケット
A	G
1600円	1600円
1	2
1600円	3200円
B	H
2000年4月1日～2000年5月31日	2000年5月1日～2000年6月30日
0円	0円

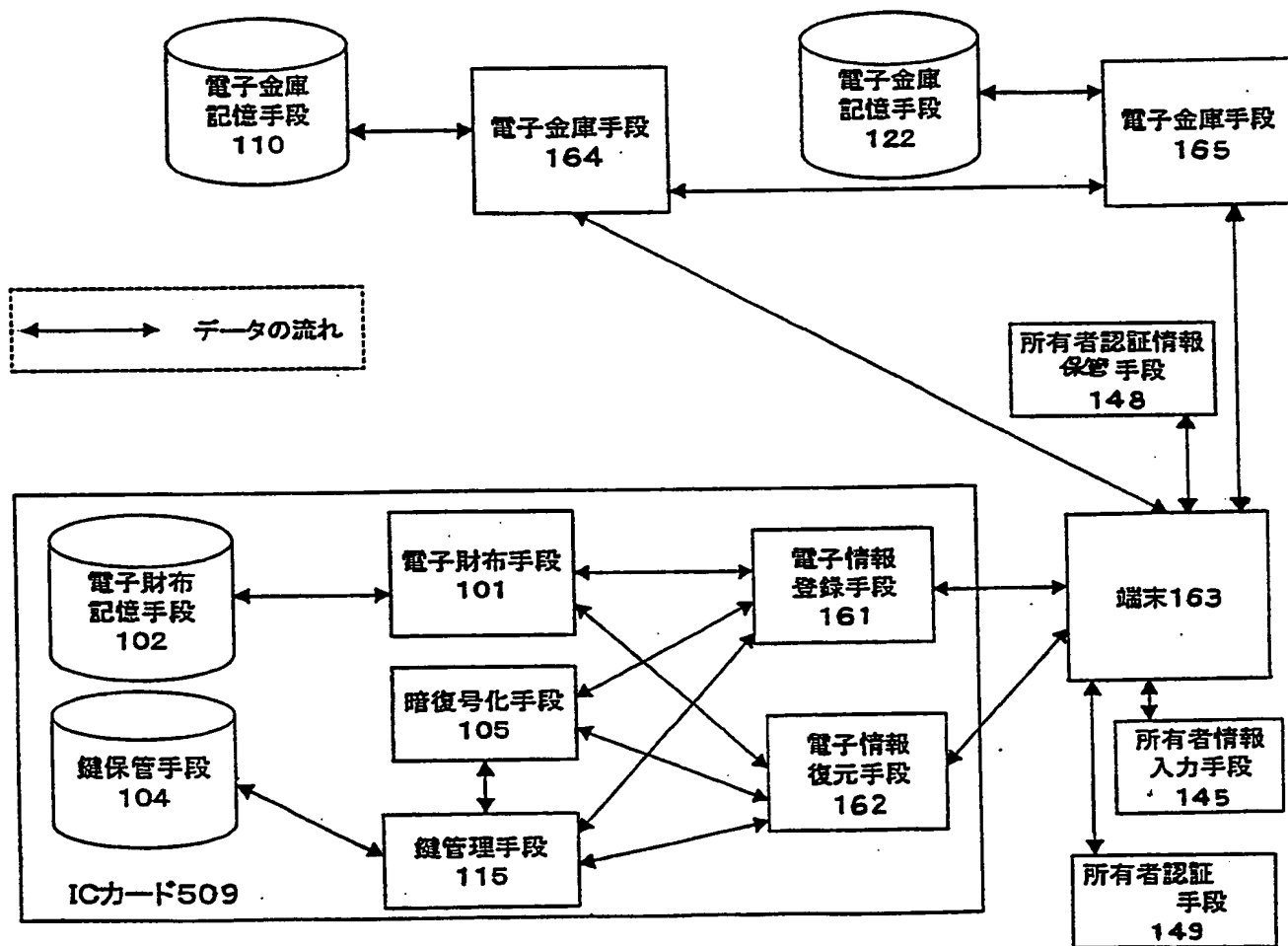
(a)

プリペイドカード	映画チケット
E	G
1000円	1600円
1	2
1000円	3200円
F	H
無期限	2000年5月1日～2000年6月30日
800円	0円

(b)

THIS PAGE BLANK (USPTO)

図 21



THIS PAGE BLANK (USPTO)

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP00/05439

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl⁷ G06F 17/60

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl⁷ G06F 17/60 G06F 19/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1926-1996 Jitsuyo Shinan Toroku Koho 1996-2000
Kokai Jitsuyo Shinan Koho 1971-2000 Toroku Jitsuyo Shinan Koho 1994-2000

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO, 96/05673, A1 (Trusted Information Systems Inc), 22 February, 1996 (22.02.96) & AU, 33217/95, A & BR, 95/08548, A & CA, 2197206, A1 & CN, 1158195, A & EP, 775401, A1 & JP, 10-508438, A & US, 5991406, A & US, 5956403, A & US, 5745573, A & US, 5640454, A & US, 5557765, A & US, 5557346, A "3. Third Embodiment - Data Recovery Centers"	27-44
X	WO, 98/35472, A1 (Connected Corp), 13 August, 1998 (13.08.98) & AU, 64342/98, A & AU, 61515/98, A & AU, 61510/98, A & US, 5940507, A & WO, 98/035306, A1 & WO, 98/035285, A2, A3 Full text	27,29-32
A	JP, 9-160990, A (Hitachi, Ltd.), 20 June, 1997 (20.06.97) (Family: none) Par. No. [0023]	1-44

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

<p>* Special categories of cited documents:</p> <p>"A" document defining the general state of the art which is not considered to be of particular relevance</p> <p>"E" earlier document but published on or after the international filing date</p> <p>"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)</p> <p>"O" document referring to an oral disclosure, use, exhibition or other means</p> <p>"P" document published prior to the international filing date but later than the priority date claimed</p>	<p>"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention</p> <p>"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone</p> <p>"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art</p> <p>"&" document member of the same patent family</p>
--	---

Date of the actual completion of the international search
07 November, 2000 (07.11.00)

Date of mailing of the international search report
21 November, 2000 (21.11.00)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP00/05439

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO, 97/02539, A1 (Hitachi, Ltd.), 13 August, 1998 (13.08.98) & AU, 63180/96, A & US, 6039250, A & EP, 241526, A1, B1 Full text	1-44
A, P	STOREY, Veda C et al., "A Conceptual Investigation of the E-Commerce Industry", in Communications of the ACM, Vol. 43, No 7, July 2000 (07.00), pp. 117-123. See the last sentence of the first section.	1-44

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl.⁷ G06F 17/60

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl.⁷ G06F 17/60 G06F 19/00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1926 - 1996 年

日本国公開実用新案公報 1971 - 2000 年

日本国実用新案登録公報 1996 - 2000 年

日本国登録実用新案公報 1994 - 2000 年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
X	WO, 96/05673, A1 (Trusted Information Systems Inc) 22. 2 月. 1996 (22.02.96) & AU, 33217/95, A & BR, 95/08548, A & CA, 2197206, A1 & CN, 1158195, A & EP, 775401, A1 & JP, 10-508438, A & US, 5991406, A	27-44

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの

「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)

「O」 口頭による開示、使用、展示等に言及する文献

「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」 特に関連のある文献であって、当該文献と他の 1 以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&」 同一パテントファミリー文献

国際調査を完了した日

07.11.00

国際調査報告の発送日

21.11.00

国際調査機関の名称及びあて先

日本国特許庁 (ISA/J P)

郵便番号 100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

阿波 進

5 L

9168

電話番号 03-3581-1101 内線 3561

C (続き) . 関連すると認められる文献

引用文献の カテゴリ*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
	& US, 5956403, A & US, 5745573, A & US, 5640454, A & US, 5557765, A & US, 5557346, A “3. Third Embodiment — Data Recovery Centers” を見よ。	
X	WO, 98/35472, A1 (Connected Corp) 13. 8 月. 1998 (13.08.98) & AU, 64342/98, A & AU, 61515/98, A & AU, 61510/98, A & US, 5940507, A & WO, 98/035306, A1 & WO, 98/035285, A2, A3 文書全体を見よ。	27, 29-32
A	JP, 9-160990, A (株式会社日立製作所) 20. 6 月. 1997 (20.06.97) (ファミリーなし) 段落[0023]を見よ。	1-44
A	WO, 97/02539, A1 (株式会社日立製作所) 13. 8 月. 1998 (13.08.98) & AE 63180/96, A & US, 6039250, A & EP, 241526, A1, B1 文書全体を見よ。	1-44
A, P	STOREY, Veda C <i>et al</i> , “A Conceptual Investigation of the E-Commerce Industry”, in <i>Communications of the ACM</i> , Vol 43, No 7, July 2000 (07.00), pp 117-123. 最初のセクションの最後の文を見よ。	1-44